NUEVA SECCIÓN: TRUCOS PARA WINDOWS VISTA

Año XI 126
4,95€

@RROBA

LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SEGURIDAD INFORMÁTICA

RICARDO GALLI

"La blogosfera es una de las cosas más cínicas y envidiosas que he visto"

HACK WIFI

Seguridad en el sistema de cifrado WEP

ASEGURA TU BASE DE DATOS

Descubre los servidores de replicación

VIRUS Y RFID

¿Puede difundirse un virus en una etiqueta RFID?

REDES ZOMBI

Cómo hacer frente a esta seria amenaza

Y ADEMÁS...

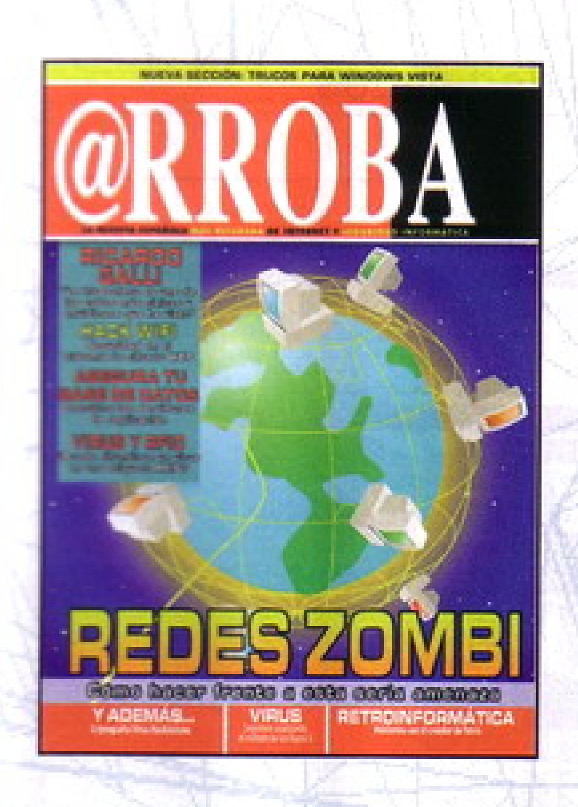
Criptografía-Crack-Hacktivismo

VIRUS

Seguimos analizando el método de los Rayos X

RETROINFORMÁTICA

Hablamos con el creador de Tetris



PRESIDENTE DEL CONSEJO EDITORIAL MARICRUZ MONTOYA LINARES/
COORDINADOR DE PRODUCCION FRANCISCO PEDREGAL BUENO/
DIRECTOR GABY LÓPEZ
REDACTORES ANDRÉS MÉNDEZ/ MANUEL BALERIOLA/ NICOLÁS VELÁSQUEZ/ SET/ SPARKRISP / MERCÈ MOLIST / PEDRO PERIS / NETTING / RAMIRO CANO / ENRIQUE ANDRADE
DISEÑO: DPTO. PROPIO
@LGARROBA DIRIGE:GABY LÓPEZ
COORDINACIÓN DEPARTAMENTO MAQUETACIÓN: GEMA BARBA
DPTO. DE SUSCRIPCIONES suscripciones@csr71.com

PUBLICIDAD: CENTRAL MEDIA YOUNG BARCELONA
AVDA. MERIDIANA 350, 5ºA - 08027 BARCELONA
TELF.: 93 274 47 39-FAX: 93 346 72 14

@RROBA
arroba@megamultimedia.com
arroba2@megamultimedia.com
Megamultimedia, S.L.
Paseo de Reding, 43, 1º
29016 Málaga
Teléfono: 952 36 31 43

DISTRIBUIDORA INTERNACIONAL
COEDIS

PRINTED IN SPAIN
III/MMVIII

ISSN-1138-1655
Dep. legal MA-1049-97 / nº126

EDUCACIÓN PARA LA SEGURIDAD

¿Tan difícil resulta hacer entender que es necesaria una educación para la seguridad informática? Desde luego, es mucho más fácil obviar la pregunta y pretender que todo se arregla con un antivirus actualizado, un firewall y cruzar los dedos por lo que pueda pasar. Y si se paga un dineral por esas soluciones, mejor. Pero la realidad es siempre más fuerte y acaba imponiéndose. No es que estemos en contra de que un usuario pague por un antivirus, al contrario. Pero pensamos que no es suficiente. Y una de las soluciones más efectivas es tremendamente sencilla, por más que se piense que es al revés. Solo hay que educarse y educar a los demás sobre lo que se va a encontrar en la Red a la hora de usarla para el trabajo o el ocio. No se arregla nada si se tiene un antivirus a la última y se entra "donde no se debe", por decirlo de alguna manera. Tampoco se trata de limitar el uso que vamos a hacer, eso sería poner puertas al campo e imponer fronteras en algo de tantas posibilidades como Internet. Pero algo va mal cuando a la hora de hablar de seguridad informática se piensa solo en ciertas medidas, y no en una educación realmente necesaria. Del mismo modo que hay prevención de riesgos laborales, ¿por qué no educar a la gente en seguridad informática, pero de verdad? ¿Por qué cuando solo unos pocos tienen que saber de qué va esto?

[SUMARIO número 126]





Arsys Internet, primer proveedor español con servidores dedicados de doble procesador Quad Core

Arsys Internet, empresa líder del mercado español de registro de dominios y alojamiento web, ha incorporado a su cartera de productos el primer servicio de hosting dedicado sobre servidores IBM con dos procesadores Intel Xeon Quad Core de cuatro núcleos. De este modo, los clientes de Arsys Internet se beneficiarán de las ventajas de estar alojados en las máquinas más potentes del mercado.

Con un alto rendimiento, los servidores con arquitectura Quad Core ejecutan más eficientemente las tareas necesarias que requieren los servicios de Internet (páginas web, correo electrónico, aplicaciones ASP...), garantizando su estabilidad y mejorando la experiencia de los usuarios finales.

Como explica Fermín Palacios, Director de Hosting de Arsys Internet, "con dos procesadores y un total de ocho núcleos, los nuevos servidores realizan un mayor número de tareas en paralelo, permitiendo que los internautas accedan a los datos más rápidamente, ya sean páginas web o complejas bases de datos. Este nuevo servicio mejorará la experiencia de los usuarios que acceden a una página web alojada en Arsys Internet".

Estos servidores cuentan con dos procesadores Quad Core, dos discos duros de 160 GB y 2 GB de memoria, entre sus principales características técnicas, y están disponibles en www.arsys.es por 222 *euros/mes. Cuentan con todas las ventajas de alojamiento que ofre*ce Arsys Internet e incluyen soporte técnico gratuito 24x7 por teléfono y correo electrónico, periodo de prueba de 30 días y garantía ilimitada del correcto funcionamiento del hardware.

Con más de 550.000 dominios registrados y más de 180.000 clientes, Arsys Internet ocupa la primera posición en el mercado español de registro de dominios y alojamiento web y se encuentra entre los primeros puestos del sector en Europa. La empresa, que emplea a más de 250 personas, presta servicios de Internet a más de un centenar de países a través de arsys.es, arsys.fr y arsys.pt.

Las líneas "Platinum", de precio reducido, también llegan a los teléfonos móviles con I-play

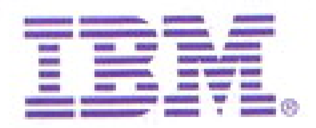
I-play, empresa líder dedicada a los videojuegos para móviles, anuncia hoy el lanzamiento de sus líneas económicas de grandes éxitos, con los títulos The Fast and the Furious Fugitive y The Fast and the Furious Tokyo en un pack 2x1.

Estos packs suponen un ahorro de mas de 4 € respecto de la compra de videojuegos tradicional, ya que el usuario no paga el gasto del segundo título y tampoco necesita de dos conexiones para descargarse dos juegos. I-play es la única editora de juegos para móviles que utiliza esta tecnología de empaquetado de juegos, lo que permite ahorrar más de 665 de las antiguas pesetas a la hora de comprar sus nuevos packs económicos de juegos para móviles.

The Fast and the Furious: Tokyo es la tercera parte de la saga conocida en España como A Todo Gas. La versión 3D de The Fast and The Furious: Tokyo Drift proporciona una nueva dimensión a los juegos para móviles, ofrece escenarios urbanos 3D, el puerto, las montañas y el viejo circuito de carreras. Otras características son la personalización del vehículo, puedes diseñar tu propio coche de carreras acudiendo a la tienda de cromados. The Fast and the Furious Fugitive fue la culminación de la saga, la última entrega de la franquicia de juegos de carreras basados en películas más exitosa del mundo, con 7 millones de descargas realizadas a lo largo de sus entregas. El jugador puede elegir el tipo de partida (Misiones o Carreras Callejeras). Una vez dentro de la partida puede realizar desplazamientos libres para cumplir misiones, carreras urbanas ilegales y persecuciones por carretera. En el juego existirán hasta 5 tipos de coches, cada uno con mandos distintos: deportivo, tuneado, gran rendimiento y exótico. Sea cual sea el que elijas, podrás elegir entre las carreras callejeras ilegales o las misiones por la ciudad para conseguir el dinero que te hace falta. Ambos juegos pueden adquirirse a un precio de 3 euros en un pack 2x1.

Puedes obtener más información de estos juegos y descargarte info, material gráfico y vídeos desde:

The Fast and the Furious Tokyo:
http://www.i-play.com.es/the_fast_and_the_furious_fugitivo-juego-42.html
The Fast and the Furious Fugitivo
http://www.i-play.com.es/the_fast_and_the_furious_tokyo-juego-25.html



Fiabilidad, escalabilidad y solidez asegurada

¿Por qué conformarse con menos? Nada mejor que el servidor **IBM System x3550** con procesadores **Intel Xeon Quad Core** y un impresionante bus frontal de **1.333 MHz**.

Gracias a su arquitectura con ocho núcleos, el procesador **Intel Xeon Quad Core**, ejecuta a gran velocidad sus aplicaciones aún en los más exigentes entornos multitarea. Al disponer de dos procesadores, el equipo puede incrementar su rendimiento siendo capaz de realizar tareas en paralelo. Y, si uno de los procesadores deja de estar operativo (bucle infinito, sobrecarga...), queda otro procesador disponible para cerrar procesos o reiniciarlos.

El **x3550** es un servidor de consumo energético eficiente, especialmente optimizado para obtener mayor rendimiento por vatio consumido.



La garantía del líder

Servicio

- Gestión remota del servidor
- Web y FTP
- Correo (POP3/IMAP/SMTP/Listas/Webmail)
- Bases de datos
- DNS personalizados
- Estadísticas gráficas de acceso al servidor
- Desarrollo de aplicaciones web propias
- Puntos de publicación multimedia

Gestión del producto

- Panel de control de gestión de Servidores Dedicados y Housing
- Cube Panel con 30 dominios de hosting incluidos
- Reinicios y reseteos
- Gráficos de ancho de banda y transferencia consumida
- Direcciones IP extras gratuitas

Seguridad

- Alojamiento en el IDC de arsys.es
- Protección del equipo mediante Firewall e IPS
- Monitorización básica del equipo
- Copias de seguridad opcional
- Seguridad garantizada por la certificación ISO 27001

Garantía / Soporte

- Alta y un mes gratis con contrato anual
- Garantía de 30 días de devolución
- Instalación y puesta a punto del servidor incluidas
- Garantía ilimitada del correcto funcionamiento del hardware
- Soporte técnico gratuito **24x7** por teléfono y/o e-mail

Soluciones a medida

Además de los modelos estándar, arsys.es diseña soluciones específicas a la medida de las necesidades de cualquier empresa: servidores dedicados de alto rendimiento, almacenamiento externo, balanceadores de red...

Llámanos y compruébalo.

222

Nunca antes un número había ofrecido tanto por tan poco

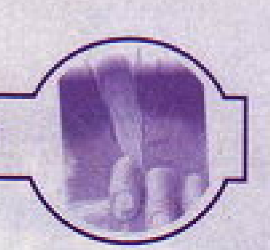




Hack wifi

Laboratorio: Seguridad en el sistema de cifrado WEP IX
Inyección de tráfico inalámbrico para la ruptura del protocolo WEP (III)
(Parte XXII)

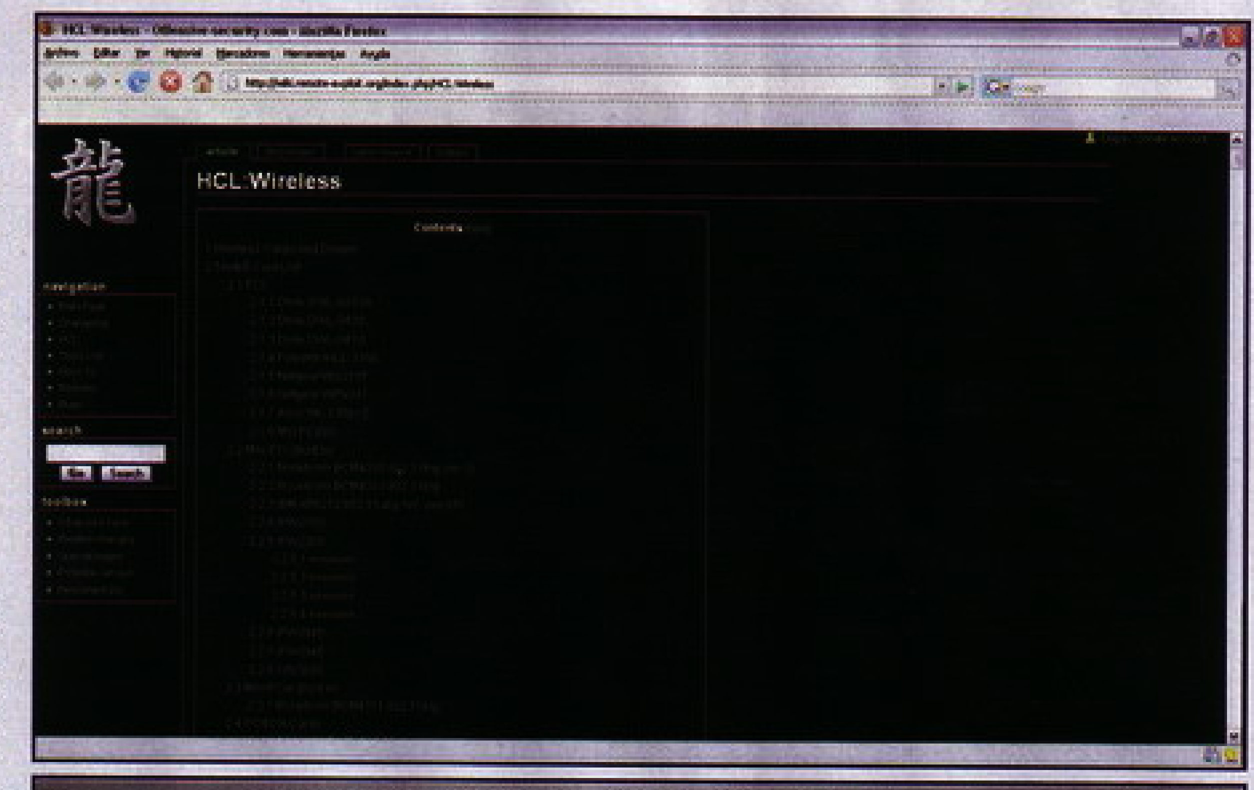
Retomamos el camino que números atrás apartábamos para un lado para hablar sobre la instalación de una red inalámbrica a medida. Con este artículo recordaremos algunas cosas de artículos pasados, os presento en profundidad algunas herramientas de una suite estupenda si hablamos de auditoria inalámbrica y definimos un poco más el rumbo de Taller Hack Wi-Fi con respecto a la inyección de tráfico inalámbrico para la ruptura del protocolo de cifrado WEP.

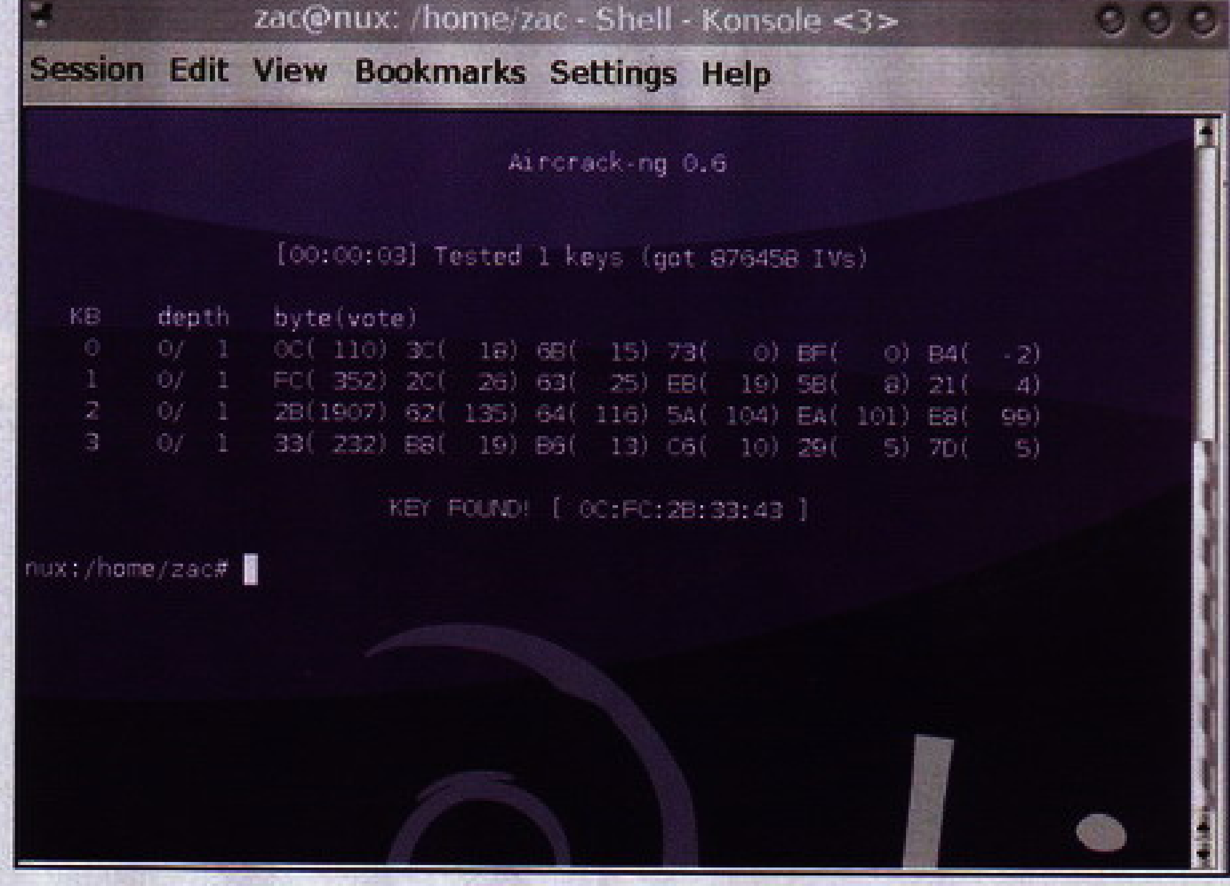


Saludos de nuevo, queridos lectores. Con este artículo retomamos el camino que perseguíamos números atrás, habíamos dejado a un lado la Inyección de tráfico inalámbrico para la ruptura del protocolo WEP para hablar sobre la instalación de una red inalámbrica a medida. Decidí hacer una pausa al rumbo del taller para hablar de un tema que me había surgido por esos meses, mejor explicar las cosas cuando están más calientas que más tarde, cuando se olvidan factores importantes.

A lo largo de estos dos últimos artículos, dedicamos el espacio y el tiempo necesario para abarcar el tema tratado. Creo que ha sido un tema interesante y que puede encaminar a más de uno en alguna ocasión aun sabiendo que la instalación de la red inalámbrica explicada era bastante específica.

Este tipo de artículos irán apareciendo a lo largo de Taller Wi-Fi cuando lo crea necesario e importante. Tengo ya alguna idea en la cabeza de una instalación inalámbrica que seguro que a más de uno pondrá los pelos de punta... quizás no por su dificultad ni por su utilidad... si no por su uso y objetivo... desde luego, hay que ser malvados...





Retomando el camino...

Volviendo al artículo de este mes. Con este artículo sumamos ya la tercera entrega de Inyección de tráfico inalámbrico para la ruptura del protocolo WEP.

Hasta ahora hemos tratado los siguientes temas:

Teoría de inyección de tráfico inalámbrico para la ruptura del protocolo WEP.

Herramientas de inyección y su funcionamiento.

Habíamos hablado algo de Aireplay, aunque no en profundidad, como se merece. Más teoría de inyección de tráfico inalámbrico para la ruptura del protocolo WEP.

Habíamos comenzado hablar de la suite aircrack.-ng.

Explicamos los pasos a seguir para instalar aircrack-ng en MS Windows.

Explicamos los pasos a seguir para instalar aircrack-ng en GNU/LiNUX.

Y por último, indicábamos algunos pasos a seguir para instalar y parchear algunos de los chipsets más usados y conocidos en nuestra distribución GNU/LiNUX preferida.

Todavía nos quedan muchas cosas que tocar. Algo de teoría que añadir y sobretodo la práctica por explicar, que seguro que la mayoría es lo que más os interesa. En la práctica expondremos variados y distintos escenarios para cubrir casi cualquier posibilidad.

Puesto que volvemos a empezar "en frío", y no quiero que se me pierda nadie, vamos hacer una breve repaso de lo explicado hasta ahora, intentaré que sea lo más práctico y sencillo posible.

Sin más preámbulos, comencemos:

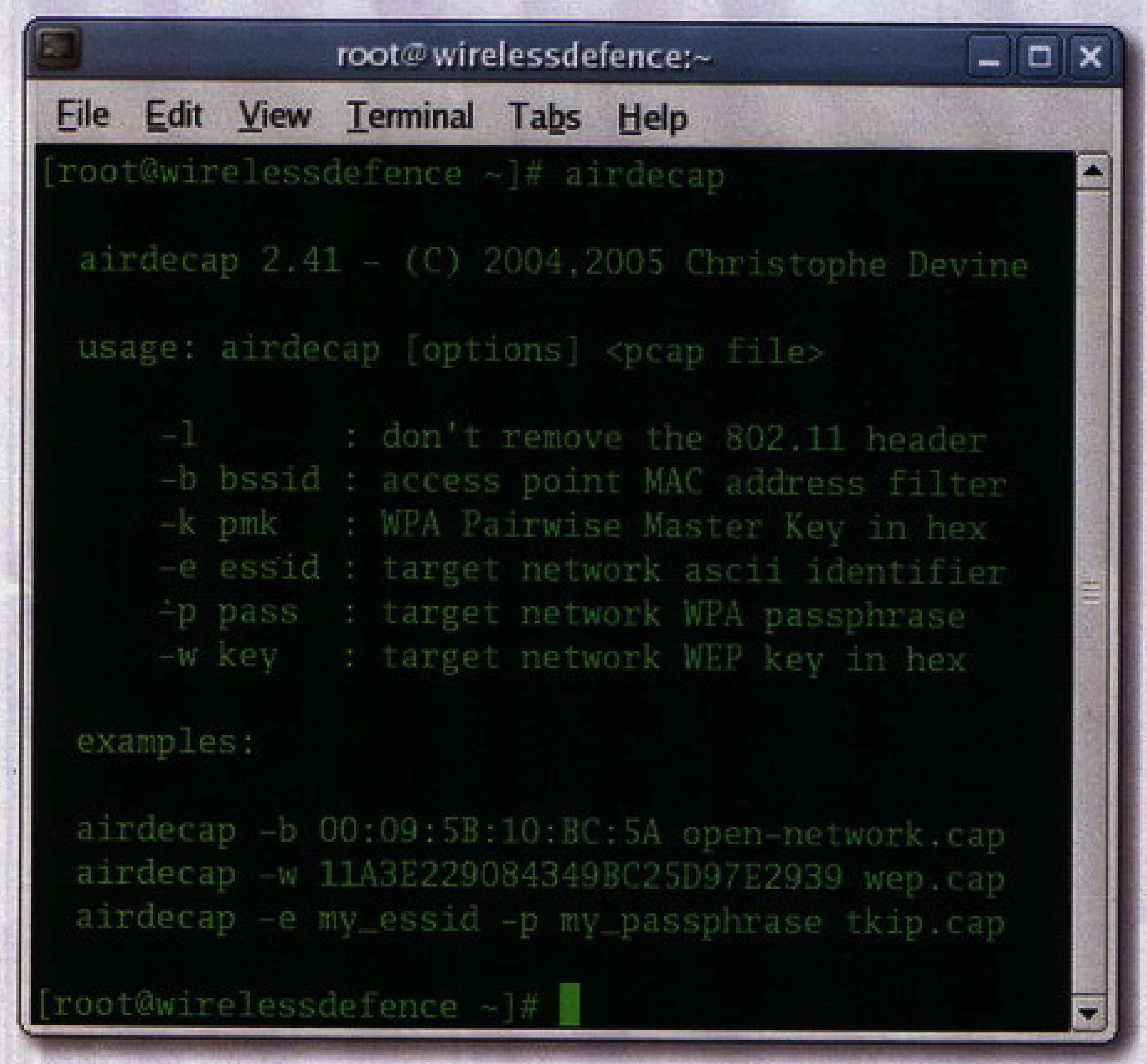
Empezando de nuevo

Antes de comenzar con el breve repaso, deciros que de ahora en adelante nos centraremos en el grupo de herramientas aircrack-ng, la suite aircrack-ng.

La suite de herramientas aircack-ng está compuesto por un analizador de paquetes, un detector de redes Wi-Fi, un crackeador de claves cifradas, y varias herramientas que nos ayudarán a analizar las redes inalámbricas 802.11 (WLANs).

Esta suite de herramientas trabaja casi con cualquier tarjeta inalámbrica cuyo controlador soporte el modo MONITOR o modo RFMON en cualquiera de los distintos Sistemas Operativos (Windows y GNU/LiNUX).






```
root@wirelessdefence:/tools/wifi
File Edit View Terminal Tabs Help
[root@wirelessdefence wifi]# airdecap -w 866578388f517be0b4818a0db1 WEP-capture-01.cap
Total number of packets read        851
Total number of WEP data packets    151
Total number of WPA data packets      0
Number of plaintext data packets      0
Number of decrypted WEP  packets    151
Number of decrypted WPA  packets      0
[root@wirelessdefence wifi]#
```

Aquí os dejo un Link la mar de interesante sobre todas las tarjetas inalámbricas soportadas, Controladores y Tarjetas inalámbricas, Lista de Testeo de Tarjetas inalámbricas, pasos a seguir para cargar los controladores de la tarjeta inalámbrica, poner la tarjeta inalámbrica en distintos modos y mucha, mucha información importante e interesante.

Vamos, que seguro que os viene como anillo al dedo. Es un sitio donde podremos encontrar muchas respuestas a nuestras preguntas.

http://wiki.remote-exploit.org/index.php/HCL:Wireless

Y para aquellos que preferís el lenguaje de Cervantes:

http://www.google.es/translate?u=http%3A%2F%2Fwiki.remote-exploit.org%2Findex.php%2FHCL%3AWireless&langpair=en%7Ces&hl=es&ie=UTF8

La suite de herramientas aircrack-ng se compone de las siguientes herramientas que pasamos a describir, me baso en la última versión disponible a la hora de desarrollar este artículo: 0.9.1:

aircrack-ng: Esta herramienta da nombre a la suite. Aircrack-ng es un crackeador de claves de redes IEEE 802.11. Puede romper varios tipos de cifrado, WEP, WPA y WPA2-PSK siempre y cuando se hayan recogido tantos paquetes cifrados como sea necesario.

Este crackeador lleva a cabo varios tipos de ataques para romper un sistema con cifrado WEP con una cantidad de paquetes determinados. Dependiendo del tipo de ataque, del tipo de cifrado, de la longitud de la clave WEP, etc. Existen ataques que requieren tan solo de un paquete con vector de iniciación, pero también existe ataques que requieren la captura de millones de paquetes con vector de iniciación para romper un cifrado con una clave WEP de 128... aunque en estos tiempos ya no suele ser muy común.

Aircrack-ng combina ataques estadísticos con ataques de fuerza bruta.

Para crakear sistemas de cifrado con WPA/WPA2-PSK debemos de utilizar un diccionario... Este es un tema que tocaremos al finalizar con el protocolo de cifrado WEP.

airdecap-ng: Con esta herramienta podremos descifrar paquetes capturados (esnifados) con alguno de los siguientes tipos de cifrado WEP/WPA/WPA2. También podríamos utilizarlo para ver la cabecera de una captura wireless sin cifrar.

airmon-ng: Viejo conocido para algunos... Airmon-ng es un script que podemos usar para poner la tarjeta inalámbrica en modo RFMON o modo MONITOR. Aunque esta no es solo su única utilidad, también nos permite trabajar con las interfaces de las tarjetas inalámbricas, salir del modo RFMON / MONITOR, ver en que estado o modo se encuentra la tarjeta inalámbrica.

Para los utilizasteis alguna vez la Live-CD Troppix seguro, seguro que habéis que tenido que tirar de este script...

aireplay-ng: Aquí encontramos la guinda del pastel si hablamos de inyectar paquetes. Este es el motivo por el cual presentamos la suite aircrack-ng, aireplay es un inyector de paquetes inalámbrico que nos servirá para adentrarnos en temas de inyección de tráfico inalámbrico para la ruptura del protocolo de cifrado WEP. Una herramienta muy útil, interesante, sencilla y eficaz.

Su función principal es generar tráfico para usarlo más tarde con aircrack-ng y poder crackear claves WEP, WPA y WPA-PSK. Hay varios ataques diferentes que se pueden utilizar para hacer deautenticaciones con el objetivo de capturar



un handshake WPA, para realizar una falsa autenticación, un reenvio interactivo de un paquete, o una reinyección automática de un ARP-request. Con el programa packetforge-ng es posible crear paquetes "ARP request" de forma arbitraria.

Si. Lo sé. Todas estas cosas os suenan a chino, todavía no las hemos estudiado en Hack Wi-Fi, pero tranquilos que pronto llegará el momento de ponerse a ello.

Como nota, recordar que la mayoría de los controladores de las tarjetas inalámbricas tienen que estar parcheados para ser capaces de inyectar. Aquí os dejo un link que trata sobre el tema de instalación de controladores:

http://www.aircrack-ng.org/doku.php?id=install_drivers

Quizás, más adelante sea un tema que abarcaremos también.

airodump-ng: Sin duda hemos llegado a uno de los pilares principales de la suite. Airodump-ng es una herramienta que utilizaremos para detectar redes inalámbricas IEEE 802.11, capturar paquetes de distintas redes inalámbricas detectadas, acumula vectores de iniciación (IVs) detectados y capturados para más tarde utilizarlos con el crackeador aircrack-ng y obtener la tan preciada clave del protocolo de cifrado WEP.



Airodump-ng es una herramienta que utilizaremos siempre cuando hablemos de auditoria inalámbrica utilizando la suite aircrack-ng.

Otra de las ventajas de airodump-ng es la posibilidad de enganchar al ordenador un receptor GPS, de esta manera es capaz de mostrar las coordenadas de las redes inalámbricas detetadas.

Sin duda será una herramienta que estudiaremos en profundidad ya que la utilizaremos para todo tipo de ataques, aunque no es una herramienta en si que lance ataques lo utilizaremos para saber que esta ocurriendo al lanzar un determinado ataque.

packetforge-ng: El propósito de packetforge-ng es crear paquetes cifrados para poder inyectarlos con posterioridad. Podemos crear varios tipos de paquetes como "ARP Requests", UDP, ICMP o paquetes hechos a medida. El uso más común es crear paquetes "ARP requests" para ser inyectados. Como veis toda una odisea :b

Para crear un paquete cifrado, es necesario tener un archivo PRGA (Pseudo Random Genration Algorithm). Este archivo lo usaremos para cifrar el paquete que vamos a crear. Este fichero se obtiene con aireplay-ng chopchop o con el ataque de fragmentación. Ataques que estudiaremos más adelante.

airtun-ng: Con airtun-ng podemos crear interfaces virtuales llamadas "tunnel interface". Tiene básicamente dos funciones:

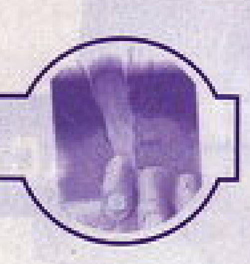
- Permite monitorizar todo el tráfico cifrado con propósitos wIDS (Wireless Intrusion Detection System. Sistema de Detención de Intrusos Inalámbrico).

- Inyectar de forma arbitraria tráfico en una red.

Para perfeccionar la captura de paquetes wIDS, debes conocer la clave cifrada y el BSSID (MAC del AP/Router) de la red a monitorizar. Airtun-ng descifra todo el tráfico de la red inalámbrica y lo pasa al sistema tradicional IDS (Sistema de Detención de Intrusos) usado por ejemplo por el archiconocido snort.

La inyección de tráfico inalámbrico puede hacerse bidireccional si conocemos la clave de cifrado completa y, solo podrá ser unidireccional, si tenemos un PRGA obtenido a través del ataque denominado chopchop o un ataque de fragmentación. La principal ventaja de airtun-ng respecto a las otras utilidades de la suite aircrack-ng es que no es la única herramienta que nos permite crear paquetes, inyectar paquetes o esnifar paquetes. Desde luego nos puede dar mucho juego. Aquí hay chicha.

La herramienta Airtun-ng solo funciona en Sistemas Operativos GNU/LiNUX.



root@wirelessdefence:/tools/wifi/aircrack-2.41

File Edit View Terminal Tabs Help

```
[root@wirelessdefence aircrack-2.41]# aireplay -0 15 -a 00:06:25:BF:64:99 -c 00:0F:3D:57:FD:C0 ath0
20:48:51  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:52  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:54  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:55  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:56  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:58  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:59  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:00  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:02  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:03  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:04  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:06  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:07  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:08  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:10  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
[root@wirelessdefence aircrack-2.41]#
```

Las siguientes herramientas citadas todavía no están disponibles a la hora de desarrollar este artículo, quizás cuando sea publicado ya se pueda acceder y utilizar las herramientas que vamos a describir:

airdriver-ng: Airdriver-ng es un "script" que proporciona información acerca de nuestros controladores Wireless de nuestro sistema operativo. Esta herramienta nos da la posibilidad de cargar o descargar los controladres. Además, airdriver-ng, nos permite instalar y desinstalar controlares completamente con los parches requeridos para el modo MONITOR o RFMON e inyección. Adicionalmente también tiene algunas otras funciones.

A continuación os pongo una lista completa de los comandos soportados por el "script":

No Command: Si Ejecutamos airdriver-ng sin ningún parámetro nos mostrará el número del kernel que estamos ejecutando y los parámetros válidos.

Supported: Este comando muestra la lista de controladores inalámbricos que el script soporta. Si el controlador que deseas utilizar no aparece listado el script no lo soporta. Hay que tener en cuenta que los controladores no estén instalados en el sistema.

Kernel: Este comando muestra los controladores inalámbricos que han sido compilados directamente dentro del kernel por el mismo.

AIRODUMP-NG ES UNA HERRAMIENTA QUE UTILIZAREMOS PARA DETECTAR REDES INALÁMBRICAS, CAPTURAR PAQUETES DE DISTINTAS REDES INALÁMBRICAS DETECTADAS...

Installed: Este comando muestra los controladores inalámbricos instalados actualmente en nuestro sistema. Aunque estes no son los controladores cargaros en el sistema

Loaded: Este comando muestra los controladores inalámbricos que actualmente están cargados en memoria.

Load: Este comando carga el controlador inalámbrico especificado en la memoria. El número del controlador se obtiene de la salida del comando "installed".

Unload: Este comando descarga el controlador inalámbrico especificado de la memoria. El número del controlador se obtiene de la salida del comando "loaded".

Install: Este comando instala el controlador especificado en tu sistema y lo carga en la memoria. El número del controlador se obtiene de la salida del comando "loaded". Todos los pasos requeridos se llevaran con cuidado, incluyendo obtener los "driver sources", parches de inyección, compilar y cargar el módulo en la memoria. Este es el modo más simple y fácil de asegurarte de que el controlador está bien instalado para poder inyectar.

Remove: Este comando borra el controlador especificado del sistema. Se borrará el módulo de la memoria y todo el árbol correspondiente del disco duro.

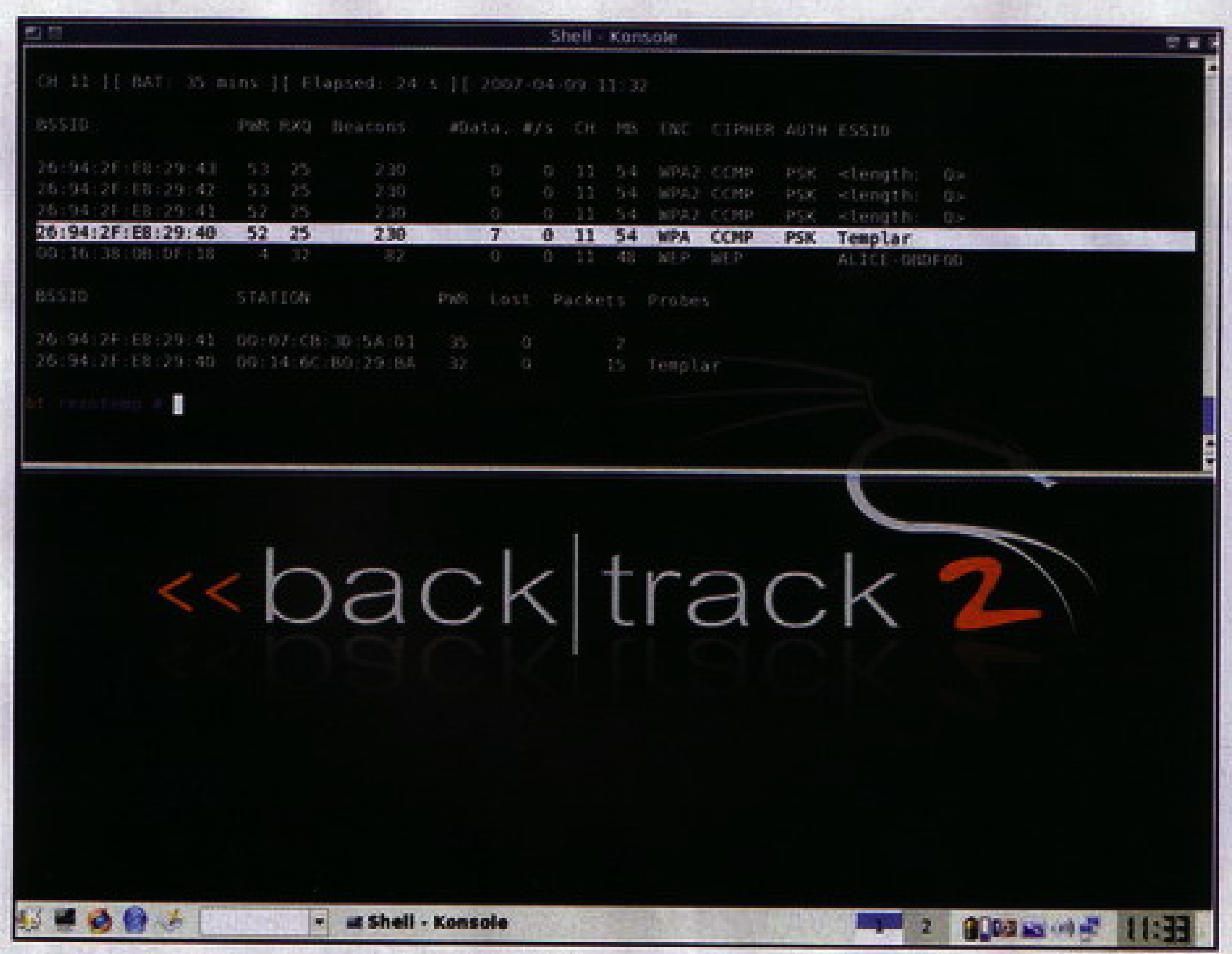
Details: Este comando muestra información detallada acerca del módulo. El número del controlador se obtiene de la salida del comando "installed". Es especialmente útil para confirmar que estamos usando la versión correcta y ver cuando fue instalada. La fecha de instalación se localiza después del nombre del archivo. Esto se puede usar para comprobar que estamos utilizando el módulo más reciente.

Detect: Este comando se usa para determinar que tarjetas inalámbricas están conectadas al PC.

No existe un método preciso para hacer estas comprobaciones. El "script" airdriver-ng solo está disponible para sistemas operativos GNU/LiNUX.

airolib-ng: Airolib-ng es una utilidad de la suite aircrack-ng para almacenar y manejar listas de ESSID y contraseñas, calcular su "Pairwise Master Keys" (PMKs) y usarlas para crackear cifrados WPA y WPA2. El programa usa la base de datos "SQLite3", que entre sus características destaca por su reducido peso, se utiliza como mecanismo almacenador que está disponible para la mayoría de las plataformas.

La base de datos "SQLite3" fue seleccionada teniendo en consideración la variedad de plataformas en las que está



soportada, memoria y espacio que ocupa en disco.

Crackear WPA y WPA2 supone calcular la "pairwise master key", que se deriva de la "private transient key" (PTK).

Calcular la PMK es un proceso muy lento ya que se usa el algoritmo "pbkdf2". Pero la PMK es siempre la misma para un ESSID y una contraseña concretas. Esto nos permite pre-calcular la PMK para conseguir combinaciones y acelerar la obtención de la clave WPA y WPA2. Los tests muestran que usando esta técnica en aircrack-ng se pueden comprobar mas de 30.000 contraseñas por segundo usando tablas PMK pre-calculadas.

Calcular la PMK todavía es un paso requerido, por lo que podemos:

- Precalcularla para usarla más tarde o compartirla.

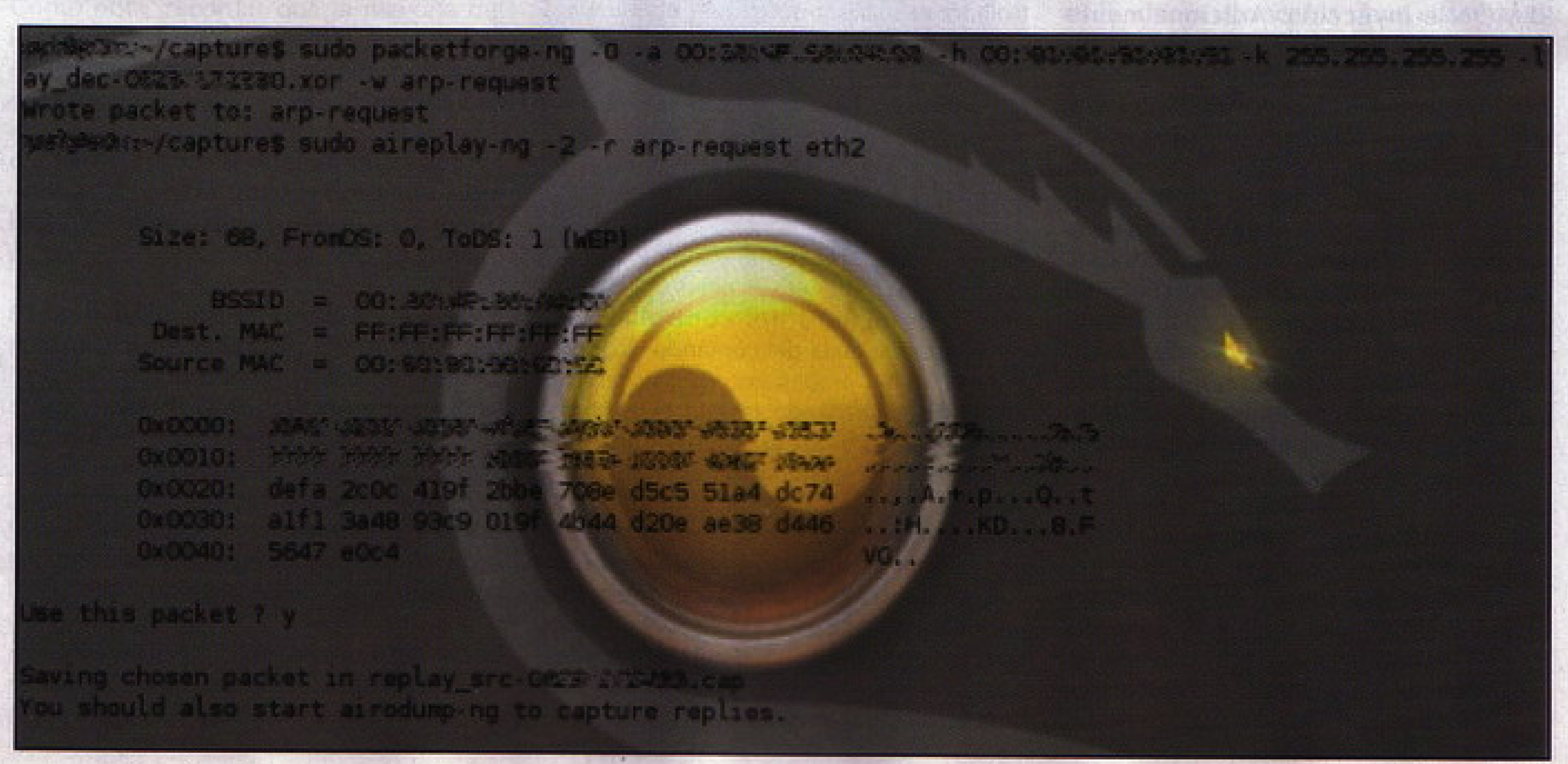
- Usar programas que generen la PMK y usen ese valor al mismo tiempo.

Como se ha dicho con anterioridad, este programa requiere la base de datos "SQLite3". Debemos ejecutar la versión 3.3.17 (o superior). Podemos obtener la última versión de SQLite de la siguiente página:

http://www.sqlite.org/download.html

airserv-ng: Airserv-ng es un servidor para tarjetas inalámbricas que permite múltiples aplicaciones y usar programas inalámbricos independientemente de la tarjeta y del controlador utilizado, a través de una conexión de red TCP basada en Cliente-Servidor. Todos los Sistemas Operativos y controladores de las tarjetas inalámbricas están incorporados dentro del servidor. Esto elimina la necesidad de que cada aplicación inalámbrica contenga los datos de la tarjeta y del controlador. También soporta múltiples Sistemas Operativos.

Cuando se inicia el servidor, escucha en una dirección IP y en un número de puerto TCP específicos por las conexiones de los clientes. La aplicación inalámbrica se comunica con el servidor a través de la dirección IP y del puerto. Cuando usemos la suite aircrack-ng, hay que especificar "<dirección IP del servidor> dos puntos (:) <número de puerto>" en lugar del nombre de la interface. Un ejemplo puede ser 127.0.0.1:666. Esto permite interesantes posibilidades:





- Eliminado la complejidad de los nombres de las tarjetas inalámbricas y de sus controladores, los desarrolladores de software se podrán concentrar en las funcionalidades de los programas. Esto permitirá que estén disponibles un mayor número de aplicaciones. También se reducen de forma importante los esfuerzos de mantenimiento.

- Sensores remotos serán de esta forma fáciles de implementar. Solo una tarjeta inalámbrica y airserv-ng se requieren para ejecutar en un sensor remoto. Esto significa que se pueden crear pequeños sistemas empotrados de forma fácil.

- Puedes mezclar y compartir varios sistemas operativos. El servidor y cada una de las aplicaciones pueden potencialmente ejecutarse en diferentes sistemas operativos.

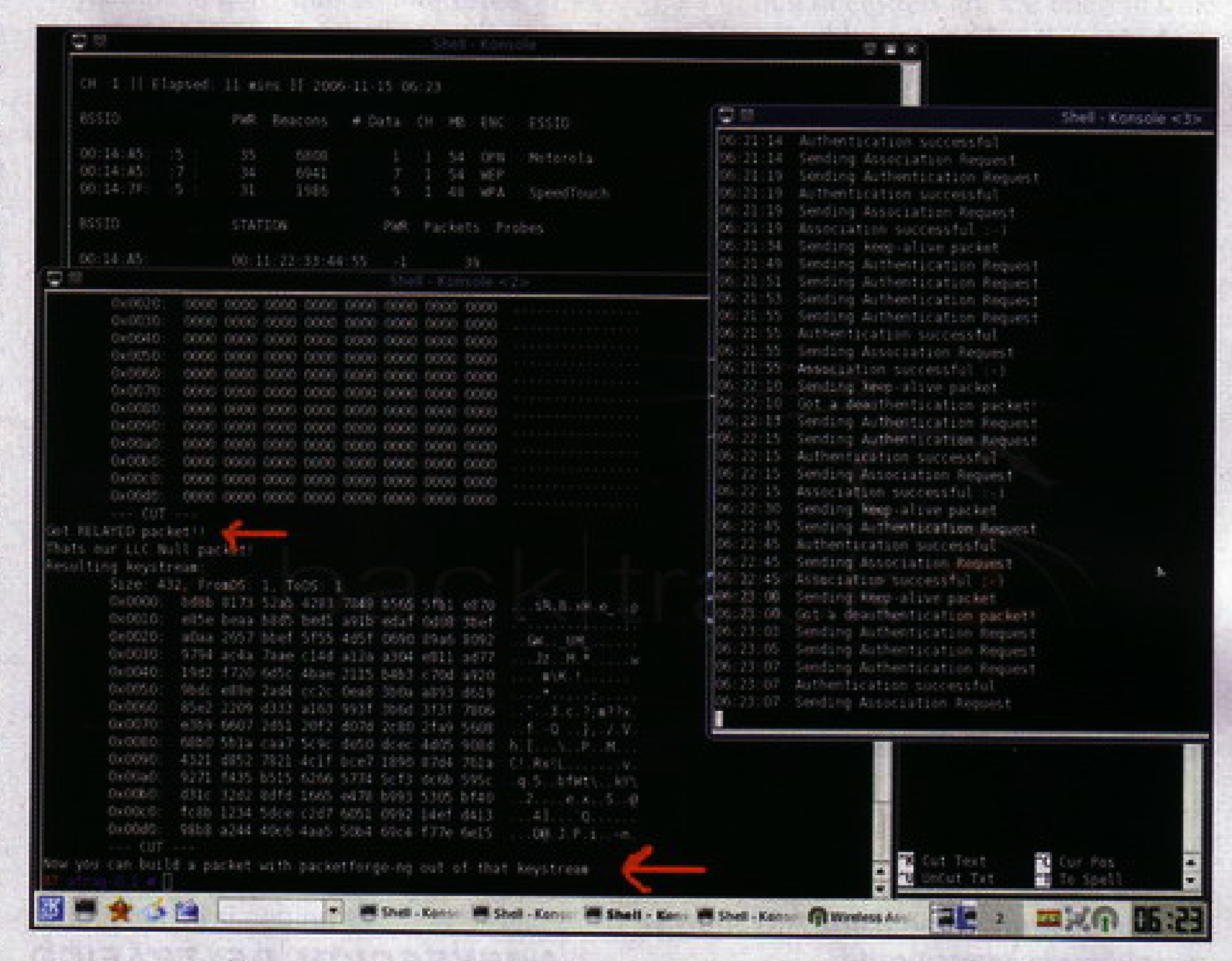
- Algunas tarjetas inalámbricas no permiten ejecutar múltiples aplicaciones al mismo tiempo. Este contratiempo se elimina ahora con este nuevo sistema basado en Cliente-Servidor.

- Usando una red TCP, el cliente y el servidor pueden encontrarse en diferentes partes del mundo. Solo es necesario disponer de una conexión de red. Funcionará sin ningún problema.

wesside-ng: Sin duda hemos llegado a una herramienta que os interesará a todos por su eficacia, automatismo, simplicidad... Es una herramienta nueva que podemos encontrar disponible en algunas distribuciones GNU/LiNUX de tipo Live-CD. Es una herramienta nueva, que algunos seguramente no conoceréis, mientras que otros seguro que ya habéis oído hablar de ella.
Wesside-ng se describe como una utilidad "auto-mágica" que incorpora todas las técnicas para obtener fácilmente una clave WEP en pocos minutos.

Primero identifica y detecta una red inalámbrica, seguidamente procede a asociarse a la misma, obtiene un PRGA (pseudo random generation algorithm) XOR DATA, determina el rango de direcciones IP de la red, reinyecta una respuesta ARP y finalmente determina la clave WEP. Todo esto lo hace sin ninguna intervención por parte del usuario. Seguro que ahora entedéis mejor lo de "auto-mágica" ;)

La utilidad wesside original fue desarrollada y creada por Andrea Bittau y fue un



programa que acompañaba a dos artículos publicados. Estos artículos son "El ataque de Fragmentación en la práctica" por Andrea Bittau y "El último descubrimiento para enterrar las redes con clave WEP" por Andrea Bittau, Mark Handley y Josua Lockey. En este links podemos ver estos artículos y muchos otros más, su lectura es obligatorio para todos aquellos que se interesen por la seguridad y auditoria inalámbrica. Estos artículos proporcionan excelente información para comprender los métodos usados para obtener claves WEP. Los conceptos para el ataque de fragmentación incorporado en aircrack-ng se han obtenido de estos artículos.

Aquí os dejo el link: http://aircrack-ng.org/doku.php?id=links

El nombre de la aplicación "wesside"? Proviene de "tupac the rapper" (2Pac / Tupac Shakur).

Wesside-ng ha sido actualizado para incluir los nuevos avances para obtener claves WEP. Los pasos que lleva a cabo wesside-ng son:

1.- Va saltando de canal buscando una red inalámbrica que utilice el sistema de cifrado de clave WEP.

2.- Una vez que encuentra una red inalámbrica, intenta autenticarse. Si la autenticación falla, entonces el programa intenta encontrar una dirección MAC que se haya asociado con el AP para engañarlo.

3.- Una vez que el programa se ha autenticado satisfactóriamente intenta asociarse con el AP.

4.- Después de esnifar un simple paquete de datos, procede a descubrir los 128 bytes de un PRGA enviando paquetes "broadcasts" e interceptando los paquetes de respuesta. Esto es lo que se conoce como ataque de fragmentación. El PRGA se escribe en el archivo prga.log.

5.-Después esnifa un "ARP REQUEST" y descifra la dirección IP usando la técnica "linear keystream expansion". Esto se usa para construir la petición ARP que se usará para la inyección.

6.- Inunda la red con peticiones ARP para esa dirección IP específica.

7.- Lanza el aircrack-ng PTW attack para determinar la clave WEP.

La técnica "linear keystream expansion" consiste en lo siguiente: El fundamento de la misma es el hecho de que los paquetes como una petición ARP cifrada pueden ser fácilmente identificados, combinado con el hecho de que el inicio de estos paquetes es texto plano. Por lo tanto el programa primero obtiene el PRGA de una porción de texto plano de la petición ARP. Después crea nuevas peticiones ARP incorrectas compuestas de dos fragmentos. El primer fragmento tiene un byte más que el PRGA conocido, por lo que el PRGA se completa con un byte extra que se intenta adivinar. Estos supuestos paquetes se envían y el programa escucha para ver cual de ellos es contestado por el AP. El paquete al que el AP contesta tiene el PRGA correcto y este valor se ha incluido en la dirección de destino "multicast". Ahora que conocemos el PRGA correcto, un byte más puede ser descifradp en la petición ARP original. Este proceso se repite hasta que la dirección IP enviada en la petición ARP original es descifrada. Esto lleva un máximo de 256 paquetes "adivinazas" para determinar el PRGA correcto para un byte concreto y de media solo 128.

Existen algunas limitaciones conocidas:

- Solo soporta autenticación abierta (open authentication). No soporta autenticación con clave compartida (Shared key authentication).

- Solo soporta redes inalámbrícas con estándar IEEE 802.11B y IEEE 802.11G.

-La funcionalidad de falsificar la dirección MAC no funciona si en la red hay mucho tráfico.

Es importante recordar que este programa se encuentra en desarrollo, por lo tanto, puede tener errores o bugs en la programación de la aplicación.

Algunas opciones puede que no funcionen como esperábamos.

Otras utilidades: A continuación citamos algunas herramientas que encontramos dentro de la suite aircrack-ng.

LA INYECCIÓN DE TRÁFICO INALÁMBRICO PUEDE HACERSE BIDIRECCIONAL SI CONOCEMOS LA CLAVE DE CIFRADO COMPLETA Y, SOLO PODRÁ SER UNIDIRECCIONAL

WZCook: Esta herramienta recupera claves WEP en PCs con sistema operativo Microsoft Windows XP, que se encuentran configuradas a través del servicio "Wireless Zero Configuration utility". Este software es experimental, por lo que puede de funcionar o no, dependiendo de la versión del "Service Pack" que tenga el sistema operativo MS Windows XP.

WZCOOK puede también recuperar la clave PMK (Pairwise Master Key), un valor de 256-bit que es el resultado de combinar la frase o "passphrase" 8.192 veces junto con el ESSID y el tamaño del ESSID. La "passphrase" no puede recuperarse en si misma - aunque, conocer la clave PMK es suficiente para conectarse a la red WPA con wpa_supplicant (en el fichero README podemos obtener más información). El archivo de configuración wpa_supplicant.conf debe ser algo parecido a:

```
network={
   ssid="el_essid"

pmk=5c9597f3c8245907ea71a89d[
...] 9d39d08e
```

Si no se utiliza el servicio WZC, pero si la utilidad de USR, podemos probar a utilizar este valor del registro here:

```
HKey_Current_User/Software/AC
XPROFILE/profilename/dot11WEP
DefaultKey1
```

Este es un tema que ya hemos abarcado en Hack Wi-Fi aunque seguro que volveremos a abarcarlo.

Ivstools: Esta utilidad une varios archivos *.ivs, Vector de Iniciación. Puedes unirlos, mediante merge o convertirlos, mediante convert.

También puede convertir ficheros *.dump de Kismet.
Pcap2ivs de algunas versiones de la suite aircrack, y aircrack-ng tiene un bug que crea capturas corruptas. No uses pcap2ivs. Si tienes un archivo con IVs corrupto por haber usado pcap2ivs, prueba a usar FixIvs para recuperarlo.

```
file:///doku.php?id=fixivs
```

Ivtools

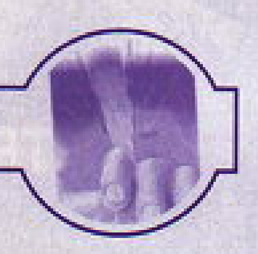
Como veis todavía nos quedan muchas, muchas y muchas temas que tocar, aprender, aplicar y con las que ensuciarnos las manos.

Con este artículo hicimos una presentación y un repaso de algunas herramientas que ya hemos citado y de otras de las que nunca hemos hablado.

Cada herramienta puede tener un mar de posibilidades y, cada herramienta le acompaña una porción de teoría. Todo ello para saber utilizarla en condiciones. El objetivo que persigo es conocer, entender y saber utilizar la mayoría de estas herramientas.

Os he ido hablando de cada uno para que nos vayan sonando términos, acrónimos, técnicas, etc. También os he puesto alga captura de pantalla que se que pondrá los pelos de punta a alguno... ¡Tranquilos! Cuando empecemos a ver todas estas cosas os resultará la mar de interesante, práctico y divertido, eso está asegurado.

Espero que poco a poco vayáis digiriendo todas estas cosas... También es cierto, que a medida que vamos desarrollando el Taller Hack Wi-Fi vamos aumentando, dentro de lo posible, el nivel del curso.



Aunque ya tocaremos el tema más adelante, cuando estemos con el barro hasta los orejas, no viene mal hablar de nuevos ataques más interesantes, rápidos y útiles... En abril de 2007 un equipo de la Universidad de Tecnología de Darmstadt en Alemania, desarrolló un nuevo método de ataque sobre la base de un documento publicado en el RC4 por Adi Shamir. Este nuevo ataque, con el nombre 'PTW ", disminuye la cantidad de vectores de inicialización (IVs) necesarios para descifrar una clave WEP y se ha incluido en la suite aircrack-ng desde la versión 0.9 liberada.

Conclusiones

Hemos presentado la suite de herramientas aircrack-ng. Suite que utilizaremos mayoritariamente en Hack Wi-Fi para el hacking, seguridad y auditoria inalámbrica.

Te he facilitado muchos links que sería recomendable que fueras leyendo, aunque no digieras la totalidad de los artículos, seguro que te viene bien ir acostumbrándote a vocablos y otros tecnicismos.

Si tienes unos conocimientos avanzados o medios seguro que te interesará lo expuestos en estos textos.

En varios artículos ya hemos tratado la instalación de la suite aircrack-ng. Por lo tanto ya no tienes excusa para tenerlas instalada y compilada en tu sistema GNU/LiNUX, incluso en MS Windows. Para los que no tenéis instalada la suite... ¡Ya estáis tardando! Y para los que la tenéis, pero se encuentra olvidada por vuestros disco duro...¡¡También estáis tardando en actualizarla!! Para los que la tenéis instalada y actualizada... pues eso, ir practicando algunas cosas, por eso del primer contacto.

Si tenéis alguna duda, tenéis algún problema de instalación, alguna duda referente al Taller, queréis información de la revista o del Taller Hack Wi-Fi como cualquier otro artículo... sabéis que tenéis a mi disposición:

Mi blog: http://blog.netting.es
Los foros: http://foro.netting.es
http://hackwifi.netting.es
http://www.wadalbertia.org (más que recomendado).

Para lo que necesitéis ahí me encontraréis para ayudaros en todo lo que pueda y esté dentro de mis posibilidades.

En el próximo número

En el próximo número en Hack Wi-Fi seguiremos con la inyección de tráfico inalámbrico para la ruptura del protocolo de cifrado WEP. Empezaremos a meternos de lleno en algunas herramientas y seguiremos con el resumen, ya un poco más denso, de lo que venimos viendo.

Aunque no tengo muy claro por donde empezar o continuar será un artículo con teoría, práctica y divertido, que también es importante.

Si no hay diversión se hace todo un poco aburrido, ¿Verdad?

Nos vemos el próximo número, aquí, en Hack Wi-Fi
Un saludo lectores ;)

nettinghxc@gmail.com
http://www.wadalbertia.org
http://www.foro.netting.es
http://blog.netting.es

"La blogosfera es una de las cosas más cínicas y envidiosas que he visto"



RICARDO GALLI: EL GRAN MENEADOR

Ricardo Galli es el Bastard Operator From Hell del fenómeno número uno de la red hispana: Menéame. Y así está, que le salen los enemigos a pares. Pero quienes conocen de antes a ese inquieto personaje ven al mismo Galli de siempre: un alma salvaje, un hacker con todas las letras, a muerte por lo que piensa. Argentino, vive en Palma de Mallorca y tiene 42 años. A sus hijas de 6 y 11 -usuarias de Linux- sólo les sorprende una cosa: que papá no esté delante del ordenador.



-¿Qué hace un argentino en Mallorca?

-Casualidad. Estaba acabando mi proyecto final de carrera en el Centro Atómico de Bariloche y vino un profesor de la Universitat de les Illes Balears (UIB) que hacía su tesis. Mi proyecto iba sobre asignación de tareas de mantenimiento de reactores nucleares.

-Uf.

-Este profesor, Arturo Fraile, vio lo que estaba haciendo y dijo: "En el aeropuerto de Palma tienen un problema de asignación de plazas a los aviones". Se hizo un convenio entre la UIB, el Centro de Bariloche y el aeropuerto para desarrollar un programa y, en verano del 91, vine a hacer las pruebas en el aeropuerto de Palma.

-¿Cómo fue que te quedaste?

-Yo quería hacer el doctorado en Informática, pero en Argentina no había. A través del rector de la UIB, Nadal Batle, me ofrecen terminar aquí la tesis y quedarme de profesor.

-¿En seguida entraste en la comunidad hacker de la isla?

-No, me metí en proyectos europeos y degeneré bastante. En Bariloche havía vivido mi época de hacker total, hacíamos bromas a los estudiantes que hacían experimentos en el reactor. Un amigo, Ignacio Fontanini, que era un cabronazo, les programaba virus para que los gráficos saliesen deformados. Era muy freak porque estábamos jugueteando con programas en un reactor nuclear.

-Juer...

-La parte del reactor ni se tocaba, pero luego estaban los aparatos de experimentos, porque era un reactor de investigación. Y cuando se encendía, aquel día estaban todos allí mirando y todos infectados con los virus de Fontanini.

-Debió ser un cambio fuerte pasar a ser profesor.

-Me metí en mucho proyecto de investigación, reuniones, burocracia, Bruselas. Era la forma que tenía para hacer mi tesis doctoral, sobre 3D colaborativo, pero me llevó mucha amargura.

-¿Y te escapaste metiéndote en BULMA?

-Teníamos chavales becarios y dos o tres estaban creando BULMA (Bisoños Usuarios de Linux de Mallorca y Alrededores). Me pidieron usar un servidor de la universidad y dije que sí. Yo llevaba desde el 93-94 dando clases sólo con Linux.

-¡Qué precocidad!

-Yo venía del mundo Unix. En Bariloche éramos muy Unix. Y cuando estudiaba en la universidad, en el 85-86, también programaba en Unix. Por eso quería dar mis clases en Unix pero tenía muchos problemas legales. También el BSD. Así caí en el Minix.

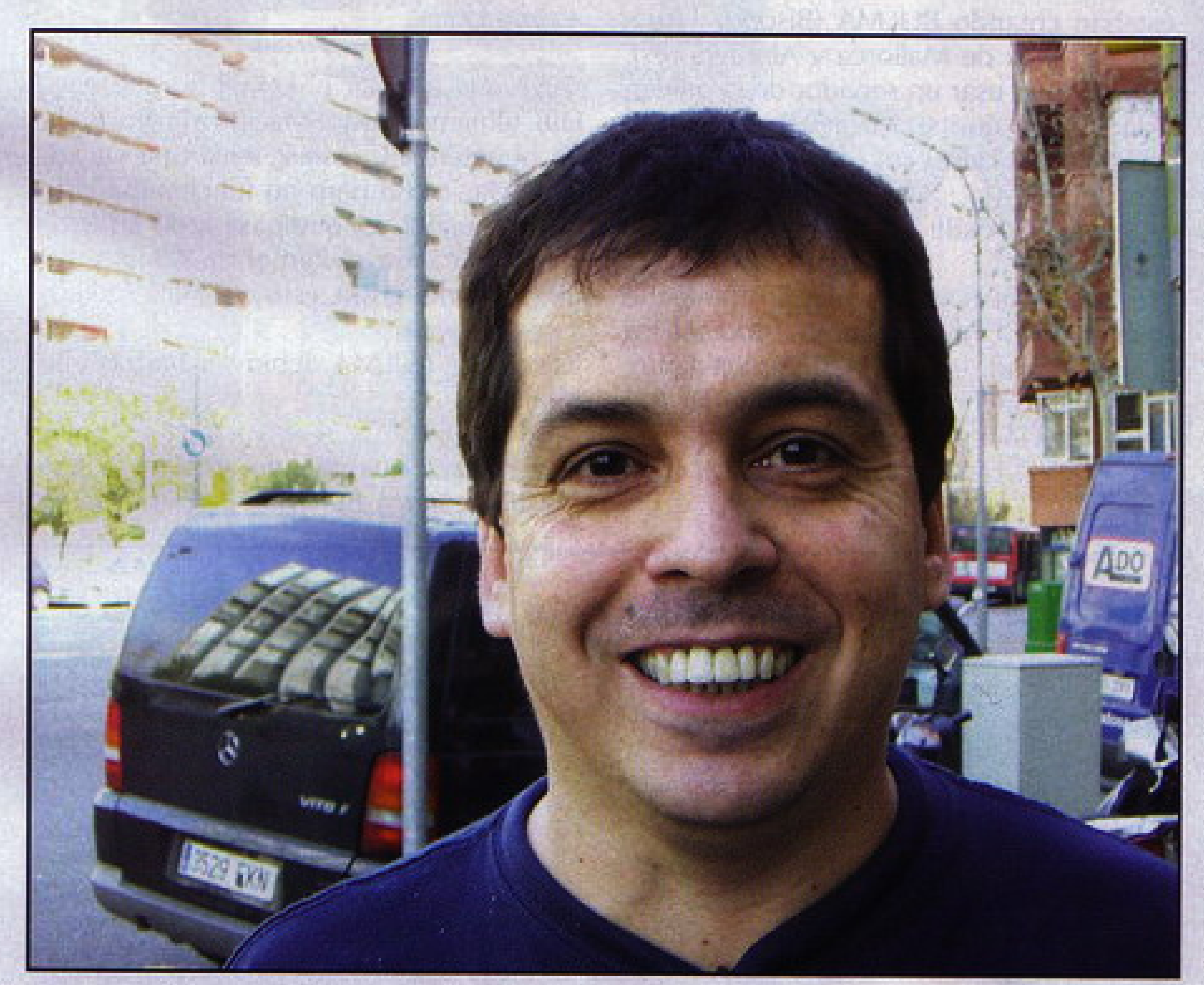
-Como Linus.

-Tuve que adaptar el kernel porque en la UIB teníamos todo Macintosh, no había un puñetero PC. Minix tenía una versión para Macintosh pero no funcionaba el teclado español, así que pasé todo un agosto modificando el kernel de Minix y me dije: Esto me gusta, esto es lo que quiero.

-De aquí a BULMA debió ser un paso natural.

-Me prometí que cuando acabase la tesis me dedicaría a BULMA. La deposité en

ENTREVISTA RICARDO GALLI



noviembre del 2000 y empecé a mejorar el gestor de contenido de la web, también implementé el sistema de RSS. Chorraditas así.

-Enseguida fuiste el alma de BULMA.

-Allí descubrí que es divertido participar en comunidades y lo complicado que son, pero sin comunidad no haces nada. En aquellos años se hablaba de BULMA por todos lados y, en realidad, éramos cuatro gatos locos.

-¿Y, un día, te cansas de BULMA?

-No. En 2004 dije que había sido presidente dos o tres años y ya era mayorcito.

-¿A Benjamí Villoslada, tu socio en Menéame, cuándo le conoces?

-El año 2000. Él conocía a Llorenç Valverde, catedrático de la UIB.

-Llorenç ha sido un poco...

-Un hub. Le dijo a Benjamí que si quería hacer cosas de software libre en Mallorca hablase con Ricardo. Me llamó una noche, cenamos y estuvimos hasta las tantas. Luego hicimos varios proyectos, como Ona Mallorca, que fue la primera radio que transmitió en Vorbis en España, en 2001.

"YO VENÍA DEL MUNDO UNIX. EN BARILOCHE ÉRAMOS MUY UNIX. Y CUANDO ESTUDIABA EN LA UNIVERSIDAD, EN EL 85-86, TAMBIÉN PROGRAMABA EN UNIX"

-¿Menéame fue idea de los dos?

-En BULMA, en el 2001, ya estábamos hablando de votar artículos y juntar los de todos los LUGs (Linux User Groups). Salió Libertonia, que venía de Kuro5hin. La idea estaba allí desde hacía años pero faltaban algunas cosillas, una de ellas que triunfase el Ajax y también encontrarle el truco, que los de Digg hicieron muy bien.

-¿Qué truco?

-Su simplicidad y la barrera de entrada muy baja. Para que saliese publicado algo tuyo en Libertonia había que escribir un cacho artículo sin un puñetero error y quizás saldría publicado. En cambio, en Digg escribes una línea, pones un enlace y ya está.

-¿Cuándo nace Menéame?

-En octubre de 2005 estaba cabreado: Coño, ¿por qué nadie lo hace en España?. Si era un regla de tres simple: Slashdot-Barrapunto, Kuro5hin-Libertonia, Digg-algo. Y nadie lo hace, serán vagos. ¿Qué pasaba? Pues que Digg no era software libre. Pensaba que sería una putada si lo hacía una empresa porque no sabes cómo va, no tienes el software... Imaginaba esta escena. Así que cojí el Puente de la Constitución y me puse a hacerlo yo.

-¿Así, a las bravas?

-Le dije a mi mujer: "Mira, tengo esta idea y creo que lo tengo que hacer".

-¿En cuánto tiempo programaste el Menéame?

-La versión básica inicial, en 12 días.

-¿Benjamí te ayudó?

-Le llamé y le dije: "Comienzo esto, ¿me echas una mano?" Y dijo que sí. Dije: "Yo iré haciendo chapucillas con el diseño y luego tú irás adaptando". Llamé también a Guillem Cantallops para que se encargase del servidor. Luego, un banco contrató a Guillem y estaba muy liado, así que tuve que coger la parte de sistemas.

-¿Cuántas horas al día dedicas a Menéame?

-Muchas más de las que debería. Algunos días sólo 4 o 5 y otros, 12 horas. La media serán 8. No veo la tele.

-¿Cobras?

-500 euros al mes, por el tema legal, para que sea compatible con mi trabajo en la universidad. La gestora nos dijo que lo mejor era hacerme autónomo y cobrar un salario. Pues lo mínimo, lo que queda después de los gastos. Además, desde enero del 2007 hemos hecho una Sociedad Limitada y soy socio y secretario.

-Cuentas en tu blog que Menéame viene de MNM.

-Del proyecto europeo Minority Newspapers for Multimedia. Valverde también estaba allí y cuando le preguntaban cómo se escribía MNM decía: "Como "menéame" pero sin las vocales", con toda la mala intención. Cuando comenzó el Menéame, yo no quería hacer nada serio, quería tomarlo de cachondeo.

-¿Qué cachondeo le ves a la palabra menéame? 0:)

.Que la gente pensaba que era un sitio porno.



-Dame cifras del Menéame a fecha de hoy.

-53.000 cuentas activas, 120.000 visitas al día y reales, 140-150.000.

-¿De dónde vienen?

-El 80% de España. El resto, países europeos y, en tercer lugar, México, Argentina y Colombia.

-Es impresionante las ganas que tiene la gente de salir en Menéame.

-Y tanto. Están contentos cuando salen y se montan conspiranoias cuando no. Están enfermos, jajaja.

-¿Te das cuenta de lo que has creado?

-Yo no soy un gran fan de la portada del Menéame que, en realidad, hay momentos que parece el "20 Minutos". A mí no me interesa el resultado.

-¿Qué te interesa?

-El proceso, ver cómo se está moviendo, la gente cómo discute, el tipo de discusiones que se montan, cómo una noticia de repente tiene tantos votos y otras mueren ignoradas en el peor de los ascos. Es muy curioso.

-¿Sabes que hay listas de correo para que la gente vote noticias del Menéame?

-Sí y están todos baneados o, cuando los descubrimos, los baneamos.

-Te imagino en tu ordenador, inventando nuevo código frenéticamente para parar a esas hordas que intentan colar cosas en el Menéame.

-Jaja, un poco es así.

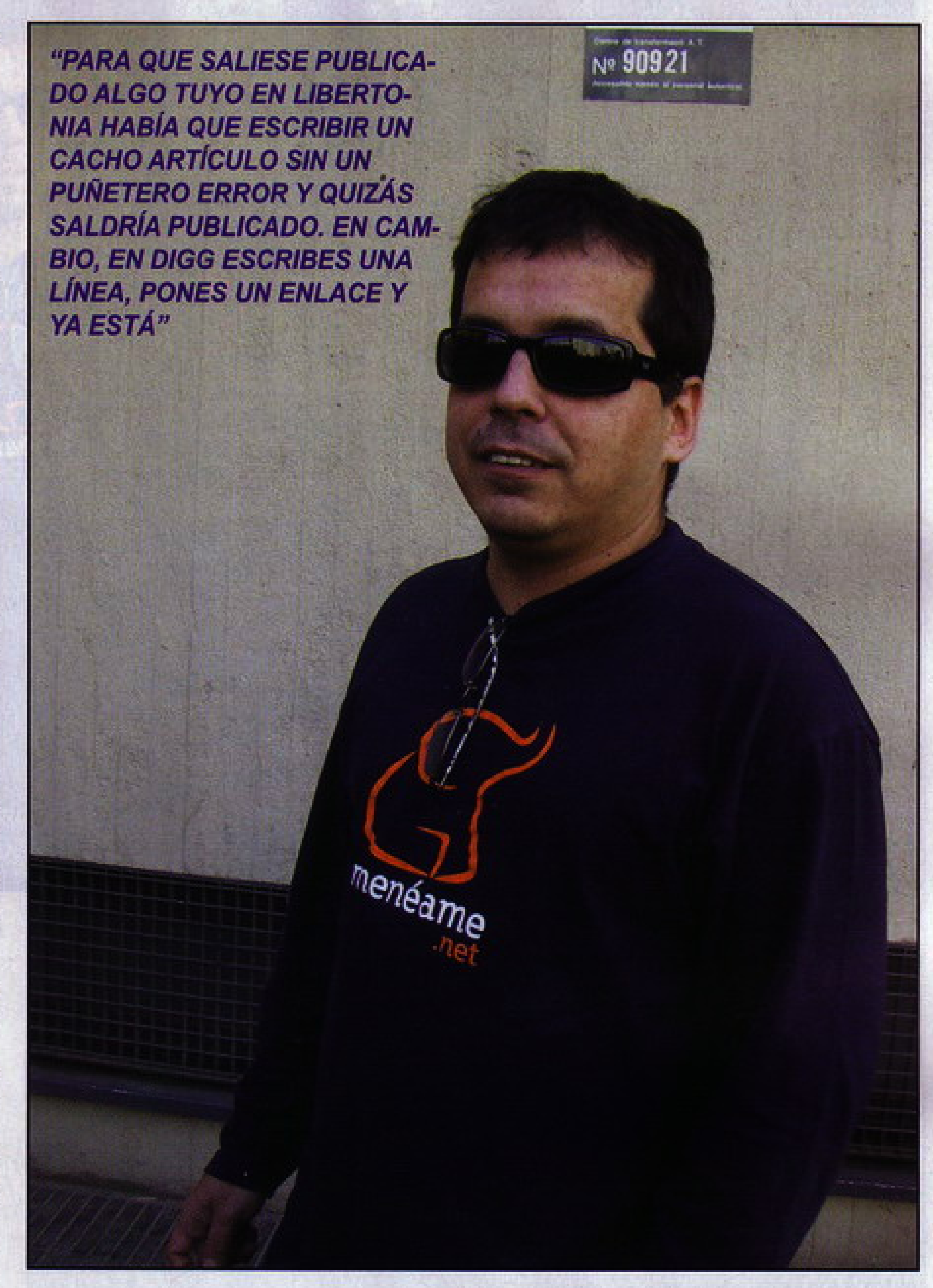
-Conozco a periodistas que harían lo que fuese para que sus artículos saliesen en Menéame.

-Y lo hacen. La mayoría de periódicos españoles, sus direcciones corporativas, están restringidos en Menéame porque se pasaban mandando cosas y votándose a ellos mismos. ¿Sabes cuáles son unos de los pocos que no están restringidos?

-Sorpréndeme.

-"El Mundo" y "Libertad Digital".

-¿Qué otros listillos hay por ahí intentando colar cosas?



-De todo, es alucinante. Unos se pasaron horas para crear más de 50 usuarios, reseteando sus "routers" para tener otra dirección IP. Otros crean sitios web con intercambio de votos. Incluso gente que usa otros dominios o los compra para que redireccionen y así poderse saltar las restricciones.

-¿Cómo los detectais?

-Tenemos dos métodos. Uno es muy eficiente: la propia gente que nos avisa. Por otro lado, tenemos una serie de scripts programados en Perl que van avisándonos de noticias con votos raros, como usuarios que todos tienen 6 de karma, lo que significa que acaban de crearlos, o usuarios distintos que comparten direcciones IP... La gente hace todas las trampas posibles, no dejan de sorprenderme, contínuamente inventan nuevos trucos.

-He leído por ahí que "Menéame ya no es lo que era".

-Sí, a los 3 días la gente ya lo estaba diciendo. Afortunadamente, Menéame cambia cada día o cada hora y depende de quien vota. Los fines de semana, cuando la gente conectada es la más friki, salen noticias más tecnológicas. Entre



"YO NO SOY UN GRAN FAN DE LA PORTADA DEL MENÉAME QUE, EN REALIDAD, HAY MOMENTOS QUE PARECE EL "20 MINUTOS". A MÍ NO ME INTERESA EL RESULTADO"

semana, más políticas. Cuando hay puentes o vacaciones, hay muchos chavales jóvenes enviando fotos, algunas de tonterías desde mi punto de vista pero es así. Lo mejor que podemos hacer nosotros es no intervenir.

-¿Ese "nosotros" es lo que algunos llaman "la mafia de Menéame"?

-Es un patrón típico de los que hacen trampas o reciben votos negativos y dicen: "Hay una mafia que me vota negativo". Yo no sé que haya ninguna mafia. De hecho, a los usuarios que colaboran les pedimos que no hablemos de noticias ni nos pasemos enlaces y que seamos muy cuidadosos de no enviar los sitios de los amigos. Y, si lo hacemos, que seamos más escépticos que de costumbre a la hora de votar.

-¿No hay mafias en Menéame?

-No. Los que lo denuncian suelen decir que tienen toda la información disponible, pero no la ponen nunca. En el Menéame intentamos, a diferencia de otros sitios, que todo sea público: votos positivos, negativos, karma, cómo se calcula. Así que sería muy fácil detectar que hay mafias y ojalá que, si se detectan, nos avisen para corregirlo.

-También dicen que hay censura.

-En Menéame nunca se ha borrado una noticia ni un comentario. Sí se han editado noticias porque incumplían las normas, como poner datos personales o insultar a una persona, pero están allí, se pueden consultar y lo que hemos hecho y el porqué están en un comentario en la misma noticia.

-¿Y censura de blogs?

-Los que están baneados, que además son bans temporales, de 3 meses máximo, 6 si es muy grave, tienen una razón para estarlo y si se ponen en contacto con nosotros intentamos explicarlo o corregirlo, también cometemos errores.

-¿Y de usuarios críticos?

-No. Lo que pasa, que yo mismo lo he detectado, es un gran activismo por parte de gente del PSOE que intentan promocionar sus noticias o las noticias en contra del PP y se votan positivamente entre ellos. Hemos tomado medidas cuando lo hemos detectado. Y también hay gente de ultraderecha que insultan con el típico "progre pro-etarra". Comentarios así reciben muchos puntos negativos, pero no lo llamaría censura sino castigo social.

-También se dice que muchos votan sin mirar, sólo para tener karma...

-Es verdad, hay gente que sólo vota las noticias preferidas para portada, pero el software de cálculo de karma penaliza fuertemente a quien vota así.

-¿Y no sería mejor pasar de este rollo del karma?

-Todos los sitios lo tienen, aunque lo llamen con otro nombre y no sea público. ¿Si no, cómo controlas que un usuario participa porque le gusta y no está ayudando a sus amigos a promocionar noticias? Todo esto se hace con un análisis de grafos, redes, clusters... y lo representamos con un número. ¿Hay otras formas? Algunos plantean lo de una persona, un voto.

-¿Y?

-Puede servir cuando te piden el DNI pa-



ra emitir tu voto, pero aquí no podemos pedirlo. Por tanto, es muy fácil engañar al sistema. El tema del spam es bastante importante y es muy duro pelear contra esto, nos lleva muchísimo trabajo. En las democracias occidentales los votos también tienen un karma, que es la Ley d'Hondt: el voto de una persona que vive en Formentera tienen un karma mucho mayor que el que vota en Madrid. Elegimos presidentes de un país basándonos en esto y, en cambio, parece que usar un karma en el Menéame rompe España.

-Hablando de romper, ¿hay mucha gente intentando hackearos?

-Tenemos ataques, algunos divertidos, otros bastante coñazos. Los más frecuentes son los intentos de Denegación de Servicio, para que el Menéame deje de funcionar. Casi cada semana tenemos ataques de Sync Flood. Afortunadamente Linux tiene un control anti-flood y, además, tenemos personas muy buenas, como Álex Concha, que nos hizo unas auditorías muy completas, o últimamente José

"LA MAYORÍA DE PERIÓDICOS ESPAÑOLES, SUS DIRECCIONES CORPORATIVAS, ESTÁN RESTRINGIDOS EN MENÉAME PORQUE SE PASABAN MANDANDO COSAS Y VOTÁNDOSE A ELLOS MISMOS"

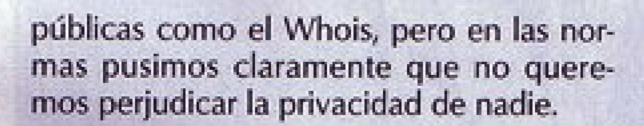
Carlos Norte, que nos pasó varios reportes de bugs en el código. Así que ahora duermo más tranquilo. Antes pensaba que nos iba a venir un ataque que nos iba a dejar en bragas. Alguna vez casi ha pasado, pero intentos serios de romper Menéame hubo antes más que ahora.

-Otro peligro es el legal. ¿Habéis tenido muchas denuncias?

-Ninguna. Hemos recibido muchas cartas de abogados, sobre todo por artículos en contra de empresas. Han llegado a decirnos que eliminemos un artículo y demos los datos del usuario o nos denunciarán. En realidad, nos están pidiendo que cometamos un delito, violar la Ley Orgánica de Protección de Datos.

-¿Qué política seguís en estos casos? ¿Borráis comentarios?

-En general no se borra nada. Lo que sí se ha hecho 3 o 4 veces es editar comentarios porque había datos personales de terceros. Seguramente en algunos casos no es ilegal, porque pueden venir de fuentes



públicas como el Whois, pero en las normas pusimos claramente que no queremos perjudicar la privacidad de nadie.

-¿Tampoco habéis borrado noticias?

-Recuerdo una empresa de Argentina que se dedicó a insultar, casi linchar, a una persona de la competencia. Sacamos el nombre de la persona y descartamos la noticia. Ha sido el único caso. En general, la gente es respetuosa, se cabrea pero sabe participar.

-¿Y la SGAE? ¿Cómo es que aún no os ha denunciado?

-Lo que es denunciable lo dirá un juez pero sí, según los parámetros de la SGAE cualquier cosa es denunciable, por ejemplo poner la fórmula SGAE = a lo que sabes, o decir que el cantante tal es un cabrón. Comentarios de esos hay muchos en Menéame.

-Por eso digo que es raro que no os haya denunciado.

-Cuando se hizo la apelación de la Frikipedia, que el Tribunal de Apelaciones de la Comunidad de Madrid volvió a dar la razón a la SGAE, empezó en Menéame una campaña de "Free Krusher". Los propios usuarios se quejaban de que otros enviasen esto, porque pondría en problemas legales al Menéame. Benjamí les contestó: "No os preocupéis y escribid lo que queráis. Tenemos dinero guardado para abogados y si nos denuncian descorcharemos un cava".

-¿Qué tal con vuestro socio capitalista, Martin Varsavsky?

-Bien. Una amiga que está en la Secretaría de Derechos Humanos de una provincia de Argentina me dijo, en agosto de 2006: Hacemos una cena homenaje al doctor Varsavsky. Ahí me acordé que, en la Noche de los Bastones Largos en Argentina, en el 96, el gobierno militar intervino en la universidad y un grupo de profesores y alumnos se opusieron. Su líder era el doctor Varsavsky. Pregunté a Varsavsky si era su padre y me dijo que sí.

-Supongo que ahí cambió tu percepción de Varsavsky, casi coincidiendo con su oferta de comprar una parte de Menéame, que primero fue el 10% y hoy es el 33%...

-Fue todo muy bien. Él, sus abogados y apoderados son unos señores. Me han tratado... El arreglo con Varsavsky fue por correo electrónico, una línea, y a partir de ahí se hizo un complejo contrato porque había que hacer ampliación de capital.

-¿Cuánto le ha costado a Varsavsky el 33% de Menéame?

-Pongamos que más de 100.000 euros.

-¿Por qué crees que le interesa?

-En una cena de bloggers, en Sevilla, alguien se lo preguntó y dijo, más o menos: "Los que están aquí tienen un alcance de llegar a la gente impresionante, más que muchos medios de comunicación. Me encanta y eso es el futuro".

"TENEMOS ATAQUES, ALGUNOS DIVERTIDOS, OTROS BASTANTE COÑAZOS. LOS MÁS FRECUENTES SON LOS INTENTOS DE DENEGACIÓN DE SERVICIO, PARA QUE EL MENÉAME DEJE DE FUNCIONAR"

-Leí que queréis profesionalizar Menéame. ¿Qué significa?

-Que alguien nos lleve la publicidad. Estamos alrededor de una décima o doceava parte del tráfico de Digg y, en cambio, Digg factura por año unos 60 millones de dólares en publicidad, mientras que nosotros no llegamos a los 100.000 euros.

-¿No te has cansado aún de Menéame?

-Estoy cansado y agobiado, pero me divierte, por eso no hemos vendido aún.

-Tenéis ofertas cada vez más fuertes, se habla de 6 millones de euros. ¿De verdad no lo venderías?

-Depende de la persona.

-Pensaba que dirías del dinero.

-No, porque no creo que nadie supere a corto plazo la última oferta que hemos recibido, muy gorda, y no hemos vendido.

-¿Te ves jubilándote aquí?

-Qué va. A no ser que cambie mucho y *sea la fuente de otras cosas.*

-¿Piensas en cambios del producto?

-Es muy difícil cambiarlo. Me gustaría buscar la forma que la gente sea más escéptica votando, que no vote tan a lo loco, pero no puedes.

-Supongo que a estas alturas ya eres un experto en Web 2.0.

-Qué va, jaja.

-¿Qué cosas buenas y malas le ves?

-Primero, que se abusa del término 2.0. También critico mucho, el otro día lo hablábamos con Emilio Márquez, que en España si tienes éxito te castigan duramente. Esto es la blogosfera-ombligosfera, que es algo muy 2.0 y una de las cosas más cínicas y envidiosas que he visto. Además de honesto tienes que parecerlo porque te van a dar por todos los lados. No creo que Digg haya recibido tantos intentos de subvertirlo.

-Menéame, el metablog, mató a Barrapunto, el blog. ¿Quién matará a Menéame?

-Si lo supiese, ya lo estaría programando :) Pero si me preguntas cómo me gustaría que sea el Menéame, una cosa que no me gusta es que la gente llega al trabajo y sigue el típico patrón: se conecta al "Marca", a "El País", "El Mundo".

-Y al Menéame.

-No, Menéame mucho menos.

-Pues mis amigos leen Menéame.

-Porque sois unos frikis.

-Jaja.

-El Menéame ahora mismo llegó a un nivel de saturación en el entorno de la gente que está mucho tiempo conectada. Poco a poco lo va superando, pero... Creció muy rápido porque creció en este entorno, pero si sales a la calle y preguntas a la gente qué lee en Internet, te dirá que El País Digital. Si preguntas si lee el Menéame dirá: ¿Qué es eso?

-Sip.

-Eso me molesta: tanto hablar de Internet y estamos leyendo lo mismo que leemos en papel. Consideraría mi objetivo cumplido cuando la gente dijese que lee "El País" y Menéame.

Mercè Mollist<

CURSO de HACKING

Nuevo recopilatorio

En esta nueva entrega de esta vuestra revista, vamos a aprender a utilizar una herramienta para tratar de descubrir las contraseñas de casi cualquier tipo de servicio.

Aquellos que se hayan incorporado recientemente a este curso habrán notado que hacemos referencia en muchas ocasiones a anteriores artículos. Esto se debe a que esta sección de la revista está orientada a modo de curso, como su propio título indica. El beneficio de ello es que no damos por supuesto que nuestros lectores tienen que venir con unos conocimientos ya adquiridos, sino que partimos de la base de que nuestros lectores no sabían nada (cuando empezamos este curso) de hacking.

Con esa idea en mente empezamos a explicar cosas muy elementales, la base del hacking para que todos nos entendieran y nadie se perdiera. Incluso pusimos una pequeña sección dentro del curso para responder las dudas que le surgían a nuestros "alumnos", con la idea de que todos aprendieran más. Algunos hackers con mayores conocimientos de los que empezamos divulgando nos tacharon de "facilones" o demasiado básicos, pero el tiempo fue pasando y nos fue dando la razón.

Y es que ha pasado mucho tiempo, 119 meses nada más y nada menos, lo que significa que el mes que viene cumplimos 10 años. Y ya sabéis lo que ocurre cuando las empresas, revistas, televisiones, etc. suelen hacer cuando llegan a una cifra semejante: unos preparan una retrospectiva, otros dan fiestas... nosotros os vamos a traer un recopilatorio.

Aquellos que llevéis poco tiempo con nosotros tal vez no lo sepáis, pero algo que nos llena de orgullo y satisfacción es el hecho de que los números de las revistas atrasadas se fueron agotando. Eso significa que cada vez que algún nuevo lector descubría esta revista, quería tener el curso desde el principio... o porque le encantaban otros artículos como los de retroinformática (entre los que me incluyo jejeje), virus, etc.





La cuestión es que los números atrasados se fueron agotando, y no queríamos perder el ánimo con el que comenzó esta sección, que jamás olvidaré. Podría decirse que cuando empezamos estábamos hartos del "oscurantismo" que rodeaba al hacking, de lo limitado de la documentación en castellano, de lo difícil que muchos querían hacer parecer la seguridad informática... y decidimos extender el conocimiento a todo aquel interesado en aprender.

Por ese motivo aparecieron los "Recopilatorios", libros cuyo contenido eran los artículos que habían ido apareciendo en las secciones. El primero que se publicó, por su demanda, fue el de Hacking, es decir, el de esta sección. En total se publicaron 3 libros recopilatorios que permitieron a nuestros fieles alumnos tener recopilados desde el artículo 1 al 54. Desde entonces no se ha vuelto a editar ningún nuevo recopilatorio... hasta este año.

Estamos trabajando en un nuevo recopilatorio que tendrá contenido inédito, y no me refiero a un "cómo se hizo", sino nuevos artículos nunca aparecidos en la revista que estamos seguros de que os encantarán. También hemos pensado en aquellos que no compraron en su día alguno de los tres primeros recopilatorios... y hasta aquí puedo leer :-)

Todavía falta algo de tiempo para su publicación, pero tranquilos porque ya llevamos meses con la preparación del mismo para que no quedéis defraudados.

¿Queréis que os avisemos cuando tengamos la fecha de publicación? Entonces mandad un e-mail a avisame@cursodehack.es y os mantendremos informados.

Nunca hables con extraños

El IRC no es algo que me haya llamado nunca demasiado la atención, cada cual tiene sus gustos, y para gustos colores. Cuando empecé a conectarme a Internet descubrí las News y para mi aquello fue mi pequeña revolución (luego aparecieron los foros, pero no acabaron con las News que siguen dando guerra). Las News permiten pensarse lo que uno postea, permiten que los demás lo lean y opinen/colaboren a la hora que mejor les venga, dejan constancia para que en el futuro la gente pueda aprender de las preguntas de los demás, etc.

Claro está que el IRC está fenomenal para poder resolver dudas en el instante, siempre que la persona que sepa respondértela esté conectada en ese momento. Pero aquí aparecen dos factores que deberían acojonar a los novatos en el hacking: inmediatez y privacidad. Me explico.

Fijaros que estoy hablando todo el tiempo de resolver dudas, está claro que quien simplemente quiera charlar un rato lo mejor es el IRC... o al menos así lo era en mis principios, luego aparecieron el ICQ, el Skype...

En las News no puedes esperar a que alguien te resuelva tu duda en el momento, con lo cual te da tiempo a pensar más sobre lo que has preguntado (¿a quién no le ha pasado el formularle una pregunta a alguien y conforme estás terminando de hablar te das cuenta tu mismo de la respuesta?), o incluso enriquecer la pregunta para que los demás te entiendan adecuadamente. Por el contrario, en el IRC la gente tiende a mandar una frase dividida en 5 mensajes, que se intercalan con los mensajes de otras 20 personas al menos... y de repente alguien te manda un privado. ¡Por fin alguien sabe la repuesta! Gracias al cielo, una persona se interesa por tu problema y se ofrece para ayudarte sin que los demás tengan que ver molestadas sus charlas con tus preguntas.

En las News, cuando alguien responde una tontería no es raro ver como otros desmienten la "chalaura" y te indican lo que ellos piensan que es lo correcto. En un privado por chat la posibilidad de contar con una tercera opinión no suele darse.

Os voy a contar un caso real para que veáis hasta qué punto podéis engatusar a alguien... o alguien puede engatusaros a vosotros.

Recuerdo un día en el que estaba conectado en un canal de IRC sobre hacking. No recuerdo cuál fue el motivo que me llevó a aquel canal, si andaba buscando ayuda o gente con quien investigar. La cuestión es que me apareció un privado de una persona que me preguntó por el Back Orifice, el troyano, buscaba a alguien que le explicara cómo usarlo. Me presté a explicárselo (yo estaba totalmente impregnado del buen rollo que había en las News por ayudar al prójimo).

Él tenía el programa, pero no se aclaraba. Le expliqué que debía desactivar el antivirus antes de descomprimir los ficheros, dado que si no el antivirus los borraría. Ahí me dio por pensar en llevar a cabo un experimento, ver hasta dónde la gente se fía de los demás. Con el antivirus deshabilitado le indiqué que ejecutara el troyano, no el cliente. Lo hizo sin reparo, sin darse cuenta de que se estaba infectando. Luego le expliqué cómo arrancar el cliente y conectarse a un ordenador que yo sabía que estaba infectado en la 127.0.0.1 (una trola que me inventé, en realidad se estaba conectando a su propio ordenador). Le expliqué en qué consistían algunos comandos, lo estuvo flipando hasta que le dije que probara el comando "shut down", que estaba genial. Dicho y hecho, a los pocos segundos desapareció del IRC, acababa de apagar su propio ordenador.

Este chico ni se planteó mirar en el buscador de la época (Google creo que todavía no había nacido) qué significaba "shut down". Tampoco se preguntó qué podía ser eso tan genial, si le llego a dar un botón que le hubiera permitido apagar un servidor de un hospital lo habría hecho sin saber lo que estaba haciendo ¡toma sistema de anonimicidad, buscarse a otro que haga por ti lo que tu no harías ni loco y encima dándote las gracias!

Aparte de las técnicas de ingeniería social que acabáis de ver que se pueden utilizar (como las que usan en la trama de la película "La Jungla de Cristal 4.0"), espero que hayáis aprendido a tomar las debidas medidas cuando habléis con extraños, que básicamente son:

- No te fíes de nadie.
- Nunca le hagas daño a nadie.
- Verifica la información, siempre que puedas.

Hay una fábula al respecto que me vais a permitir que os cuente ya que seré breve. A un pajarillo le pilló desprevenido una helada, con la mala suerte de que no pudo refugiarse a tiempo. Tendido en el suelo, viendo su hora llegar, pasó por encima de él una enorme vaca que, en ese momento, tuvo a bien defecar sobre nuestro lindo pajarillo. ¡Menuda putada, se le acababan de cagar encima! Afortunadamente pasaba por allí un zorro que, viendo la situación, se acercó y le lamió para quitarle la mierda que le bañaba. ¡Menos mal, aquel zorro le iba a librar del excremento! Pero, cuando el pajarillo se había quedado calentito gracias al mojón recién hecho y limpio gracias al zorro, el zorro se comió al pajarito.

Moraleja: ni todos los que se cagan en ti te están perjudicando, ni todos los que te ayudan te están salvando.

Descubriendo la clave de un LDAP... o de lo que se tercie (I)

En la anterior entrega os explicamos cómo acceder a un servidor LDAP público, ¿pero qué pasa si no es público? Siempre cabe la posibilidad de que intentemos localizar un punto débil, y las claves son un buen lugar por donde empezar.

Lo que os vamos a proponer y a explicar es el uso de una herramienta para crackear claves on-line, es decir, mediante fuerza bruta (prueba y error) pero sin disponer del fichero de claves a romper. Lo fastidioso de este método, como ya sabéis, es el tiempo que lleva hacer las pruebas, pero como le dijo el perro al hueso "Tu estarás duro, pero yo tengo tiempo".

En la entrega 80 os explicamos cómo utilizar el AccessDiver para atacar la clave de las páginas web. Dado que en esta ocasión estamos hablando de un servidor LDAP, tendremos que utilizar otra herramienta: el Brutus - Authentication Engine Test versión 2.

Lo simpático del Brutus es que lo podemos configurar de manera que se conecte a cualquier sistema que solicite usuario y contraseña y se ocupará de ir introduciendo las combinaciones hasta dar con una válida... o hasta que nos hartemos. No vayáis a pensar que se basa en un complejo mecanismo, ¡nada más lejos de la realidad! Aquellos que configurarais un Linux en la época de María Castaña, es decir, allá por el 98, os acordaréis seguramente del script que había que editar para conectarse a Internet mediante modem. El script debía entender la petición de Infovia donde nos preguntaba por nuestro login y password. Dicha solicitud era como si de una sesión telnet se tratara, es decir, que el servidor del ISP nos mandaba:

login:

y tú introducías a continuación tu nombre de usuario.

Tu script debía tener la palabra que tenía que esperar para introducir el login, es decir "login:". Pero había una cosa simpática, los scripts omitían la primera letra, pues a veces se perdía en la conexión, así se solía configurar el script de forma que esperara la palabra "ogin:". Pues bien, ya veréis como este mismo mecanismo es el que emplea Brutus.

Tras esta breve introducción, pasemos manos a la obra. Descomprimid el Brutus de brutus-aet2.zip y ejecutad brutusa2.exe. Primero os voy a explicar cómo se crackearía la clave de una página web de forma similar a como ya hicimos en la entrega 8, o sea, de aquellas páginas web donde la autenticación no es en un formulario sino en un pop-up, de esta forma entenderéis el uso básico del programa para que podamos pasar luego a la explicación que nos interesa.

Lo primero sería introducir la IP de la web cuya clave fuéramos a localizar en el campo "Target". En "Type" indicamos el tipo de servidor que vamos a crackear, en este caso seleccionamos "HTTP (Basic Auth)". En "Connection options" dejamos el puerto al que se conectará, "Port", como 80. El número de conexiones en "Connections" no es necesario que lo modifiquéis, si decidís aumentarlo irá más rápido, pero puede llegar a saturar vuestras conexiones. Con respecto al tiempo de espera entre conexión y conexión, dejar el "Timeout" por defecto, si se reduce irá también más rápido, pero se pueden perder respuestas y podríamos dejar de descubrir la clave adecuada.

Si queréis anonimizar el ataque podéis marcar la opción "Use Proxy", en cuyo caso tendríais que pulsar en "Define" para especificar los datos del proxy a emplear.

Ahora llegamos a las opciones específicas del protocolo en el que está el servidor, en este caso "HTTP (Basic) Options". El método de conexión, "Method", es mejor que lo cambiéis a GET. La opción de "KeepAlive" la podéis dejar marcada para reutilizar las conexiones, así aceleramos las pruebas.

Entramos ahora en la sección de las opciones de autenticación, "Authentication Options", donde indicaremos el usuario /usuarios a crackear. Dado que esta es una "prueba de concepto", digamos que atacaremos la clave sólo del usuario "admin", un usuario muy común jejeje (por

Brutus - AET2 - www.hoobie.net/brutus - (January 2000)
File Tools Help
Target 127.0.0.1 Type HTTP (Basic Auth) Start Stop Clear
Connection Options
Port 80 Connections 10 Timeout 10 Use Proxy Define
HTTP (Basic) Options
Method HEAD KeepAlive
Authentication Options
Use Username Single User Pass Mode Word List
UserID administrador Browse Pass File words.txt Browse
Positive Authentication Results
Target Type Username Password
Located and installed 1 authentication plug-ins
0% Timeout Reject Auth Seq Throttle Quick Kill
Idle

Pantalla principal del Brutus



desgracia para vosotros el administrador suele tener una clave más en condiciones que el resto de usuarios).

Para ello tendremos que marcar "Use Username", de forma que el programa sepa que tiene que introducir el usuario (hay webs que sólo piden la clave). Además, dado que vamos a comprobar la clave sólo del "admin", deberéis marcar "Single User", para que se centre en ese usuario exclusivamente, cuyo nombre tendréis que introducir en el campo "UserID".

Llegamos ahora a la clave, "Pass Mode", donde tenemos tres opciones:

- Word List: Prueba las palabras que haya en el diccionario que le indiquéis en "Pass File".

- Combo List: Carga el diccionario que le indiquéis en "Combo File", con la salvedad de que en cada línea del diccionario debe haber un nombre de usuario y una contraseña separados por un delimitador de los disponibles en "Delimiter". Esta opción no es compatible con probar la clave de un solo usuario, a no ser que dicho diccionario siempre ponga como usuario "admin" en cada línea.

- Brute Force: Os permite probar claves generadas en tiempo real. Para configurar el contenido de cada clave debéis pulsar en "Range".

En la nueva ventana podéis indicar el tipo de caracteres a usar ("Digits only", "Lowercase Alpha", etc.), así como el número mínimo y máximo de caracteres. La verdad es que es muy customizable.

Para la prueba que estamos llevando a cabo, nos conformaremos con la opción "Word List". Si no os parece suficiente la wordlist que trae el programa, o si necesitáis hacerle unos arreglillos, debéis acceder a Tools ➠ Wordlist Generation.

Ahí os aparecerá una nueva ventana en la que, en función del "Action" seleccionado, así funcionará. Las opciones que hay son:

- Convert list (LF>CRLF): Permite convertir un fichero de texto plano en Linux a Windows. Esto se debe a que en Linux el fin de línea y retorno de carro se representan como "LF", mientras que en Windows es "CR+LF", de ahí que hayáis visto en alguna ocasión ficheros de texto idénticos en contenido pero de distinto tamaño, ya que los de Windows usan más caracteres (estos caracteres no son visibles).

- Only word length: Saca de un diccionario aquellas palabras que tengan la cantidad de caracteres que le indiquéis entre el mínimo ("Min") y el máximo ("Max").

- Remove duplicates: Guarda el diccionario quitando las posibles palabras repetidas.

- Permutations: Dado un diccionario, permite convertir las palabras a mayúsculas ("Upper case"), minúsculas ("Lower ca-

>>> Website del mes

¿Queréis saber cuáles son las vulnerabilidades que más se están utilizando? Esta información es útil tanto a los administradores, para protegerse, como para nosotros, para saber qué es lo que se cuece en el mundillo.

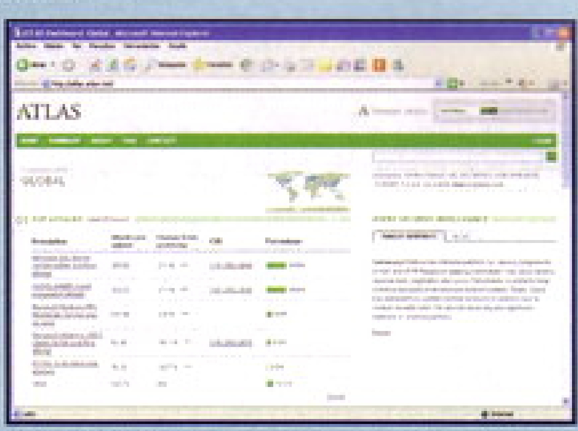
La forma de conocerlo es accediendo al servicio **ATLAS** (Active Threat Level Analysis System) de la empresa Arbor Networks. Este fabricante, según el mismo informa, proporciona la plataforma de detección de anomalías implantada en el 70% de los ISPs, lo que les permite revisar el 80% del tráfico de Internet. Gracias a esta información correla los datos con las vulnerabilidades conocidas e incluso con sus códigos CVE correspondientes.



Website de Arbor Networks

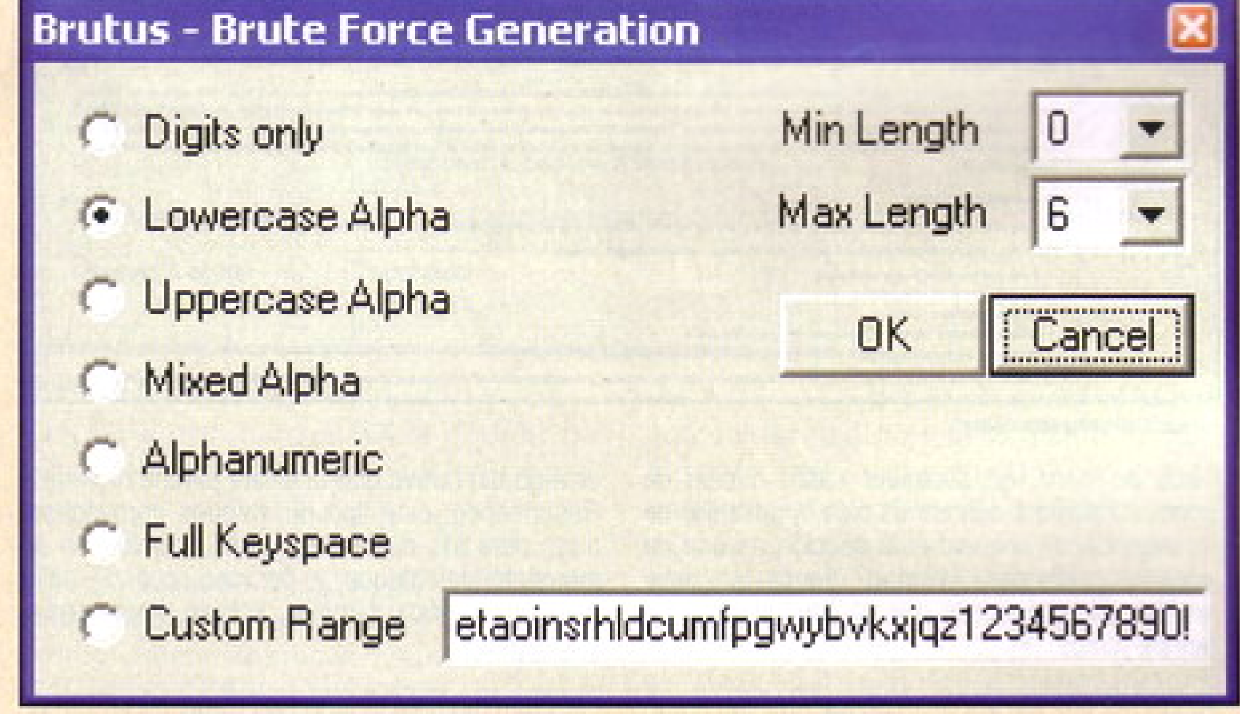
La página es accesible en **atlas.arbor.net.**

Una vez pulséis en una vulnerabilidad, podréis ver datos sobre la misma como IPs que más ataques producen, puerto que utilizan, redes objetivo, gráficas sobre la evolución, etc. Así que ya sabéis, cuidadín con lo que hacéis porque hay miles de "ojos" observando...



Información de ATLAS

ATENCIÓN WEBMASTERS: Si creéis que vuestra web (bien sea independiente o de un grupo) es lo suficientemente buena como para aparecer en esta sección, y su contenido se refiere al hacking que aquí tratamos, no dudéis en hacérnoslo saber a la dirección cursodehack@megamultimedia.com.



Opciones de las claves con fuerza bruta

Bugy Bugy

El mes pasado vimos cosas muy variopintas que iban desde MySQL a Apple pasando por el archiconocido Internet Explorer. Para que ninguno de los fans del software abierto o privativo dijera que le damos caña a ciertos programas, a los que ellos son más afines. Este mes vamos a hablar de un tipo de ataque y de bug que hace las delicias de todos los que juegan con esto de la seguridad porque les posibilita entrar en sitios antes que nadie y sin que nadie se percate de ello normalmente. Como siempre, si queréis saber más, tendréis que seguir leyendo porque hasta aquí os podemos contar.

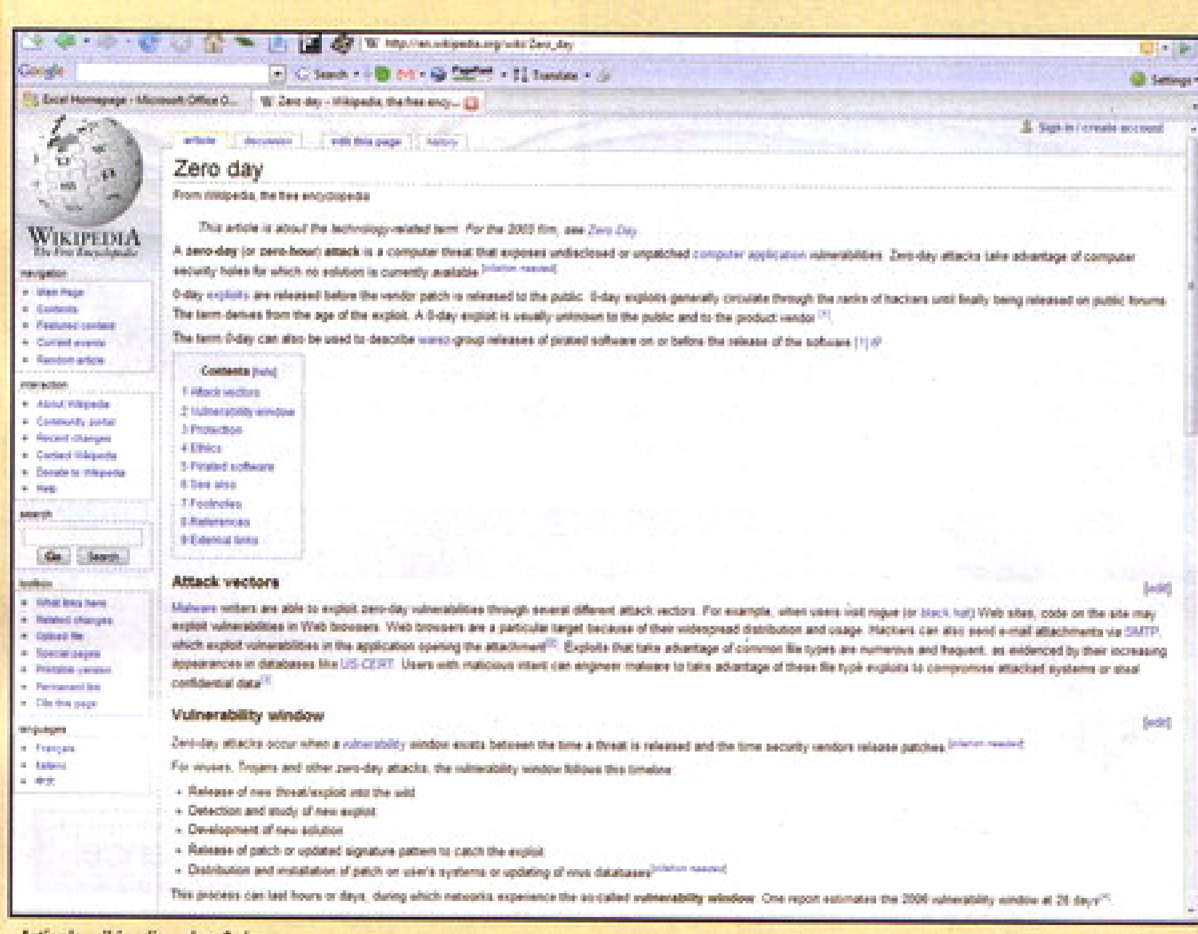
3, 2, 1,...

Este mes vamos a empezar hablando de una cosa que a algunos puede que os suene y a otros no pero, en cualquier caso, debéis de conocer, máxime cuando os pica el gusanillo de la seguridad y por eso esta sección es una de vuestras preferidas, ¿verdad? Venga, no seáis tímidos en reconocerlo que ya llevamos mucho tiempo juntos :-P.

Si alguna vez habéis visto en las noticias cómo los muchachos de la NASA lanzan un cohete al espacio, o como celebran la llegada del año nuevo en algunos países donde las uvas no se estilan, habréis visto más de una vez la importancia de una cuenta atrás. Y eso nos lleva al punto más importante de las cuentas atrás, el cero o momento de algarabía colectiva que indica que la cuenta se acabó. Como nosotros en esta sección nos ocupamos de la seguridad y estamos hablando del momento que ocurre cuando se acaba la cuenta, vamos a hablaros de su equivalente en el terreno siempre divertido de los bugs. Cuando un bug está calentito, calentito, circulando por el ciberespacio, entonces se le conoce con el nombre clave de 0-day.

Un poco de vocabulario

Sobre el término 0-day existe toda una familia de términos. Por ejemplo, si escucháis "ataque 0-day" significa que para atacar a un ordenador se va a utilizar una vulnerabilidad que tiene el mismo que, o no está documentada convenientemente, o bien está sin parchear (generalmente es algo tan nuevo que ni existe parche ni nada). Resumiendo, este tipo de ataques aprovechan bugs para los cuales no existe solución en el momento del ataque y, por eso, cuando sale alguno un poco famoso, cobran importancia enseguida.



Artículo wikipedia sobre 0-day

Otro término relacionado con 0-day es el "0-day exploit". Este término es el complemento perfecto para los ataques 0-day. Un exploit es un código que sirve para explotar una vulnerabilidad del tirón, es decir, en vez de tener que ir tecleando a mano diferentes comandos o trucos para lograr que un sistema se rinda a una vulnerabilidad, los exploits facilitan la tarea de manera increíble porque casi se podría decir que es un "ejecutar y listo". Así pues, ya os podréis estar imaginando que es un "0-day exploit". Efectivamente, es un programita que permite aprovechar un bug no parcheado o no documentado para lanzar un ataque 0-day.

Adivina, adivinanza

Llegados este punto y después de haberos introducido los conceptos básicos sobre el tipo de vulnerabilidad más sensible, seguro que estaréis deseosos de saber para quién va dedicado el artículo de este mes. Venga, no digáis ahora que eso no es cierto porque ya nos conocemos y vosotros sabéis que si os contamos una historia previa es porque detrás viene algo relacionado con eso y, además, nosotros sabemos que lo sabéis.

Por favor, redoble de tambores para darle un poco de emoción al momento. El culpable de que este mes hayamos hablado del 0-day es... Microsoft Excel. Ejem, ahora es cuando mostráis los signos de alegría o tristeza según corresponda al bando que hayáis elegido en esto de las plataformas, sistemas operativos y demás historias del lado oscuro y la fuerza jedi.



Web de Excel

Las versiones afectadas por el ataque 0-day descubierto son las versiones antiguas de Excel. Claro que lo que Microsoft denomina antiguas no siempre lo es y, por eso, puede ser que dichas versiones sean usadas todavía por un gran número de usuarios. Dichas versiones son Excel 2003 SP 2, 2002, 2000 de Windows y la versión 2004 para Mac. Para que el ataque sea exitoso, la víctima sólo tendría que abrir un fichero Excel creado para la ocasión, si eso sucediera, el atacante obtendría los mismos privilegios en el sistema que el usuario.

Así pues, nos despediremos diciendo lo que decimos siempre pero no por ello debéis ignorar el mensaje. Actualizad, actualizad y manteneros actualizados siempre que podáis al máximo.



se"), poner en mayúsculas sólo la primera letra ("First character upper case"), invertir el orden de las letras ("Reverse"), transformar letras en números ("leet speek"), añadir caracteres al final de la palabra ("Append strings", introduces o seleccionas dichos caracteres en la casilla la derecha), al principio ("Prepend strings"). Esto es muy útil cuando habéis obtenido palabras de una web o datos de alguien que pueden ser utilizados por una persona para componer su clave.

- Create new list: Genera una lista de palabras realizando combinaciones con las opciones de antes sobre las palabras que le indiques en "Seed word", puedes añadir ("Add") cuantas palabras quieras y luego las utilizará (si te equivocas puedes borrar una palabra pulsando en "Delete" o limpiar la lista de palabras con "Clear all"). Esta opción viene de perlas cuando quieres probar todas las combinaciones del nombre de alguien, a ver si es su clave, que es muy típico.

- Create new list for user: Genera un combo-diccionario (que contiene líneas con "usuario:clave"). En la casilla "Username" introduce el usuario y en "Seed word" las palabras que quieras que utilice como clave, nuevamente según las opciones que hayas elegido en "Permutations" así saldrá el nuevo combo-diccionario.

- Create new list for users: Idem que el anterior, pero para un listado de usuarios.

En la casilla aledaña "Input list" tenéis que indicar el fichero a procesar y en "Output list" el fichero donde guardará el resultado. Una vez todo configurado pulsad en "Action" para que comience el proceso.

Bueno, pues ya está todo listo para pulsar en "Start" y dejar que la informática haga el resto ;-) Si cae la clave aparecerá en "Positive Authentication Results".

Durante un crackeo, el botón "Start" se convierte en "Pause", por si queréis detener las pruebas en un momento y continuar más adelante. Claro está que para hacer eso tendréis que guardar el estado en el que se encuentra durante la pausa. Para ello id a File ➠ Save session. Cuando queráis seguir con el ataque, tendréis que arrancar el Brutus y, antes de pulsar nada, id a File ➠ Load session.

Brutus - Word List Tools

Action	Convert list (LF>CRLF)	Input list		Browse
Word length Min 0 Max 15		Output list		Browse

Convert the input list from UNIX style to DOS style line breaks — Action — Cancel

Idle

Generación de wordlists

Brutus - Authentication Sequence Definition

☑ Use pre-auth ☐ No UserID — OK — View — Cancel

Pre-authentication sequence
- Selected pre-authentication phase: Pre-auth phase 1
- Target response string:
- Force read of at least 1 bytes of target response
- Brutus send string: None

Authentication sequence
- Selected authentication phase: UserID phase
- UserID prompt:
- Force read of at least 1 characters of target response
- UserID format: UserID — None

Response sequence
- Selected target response string: Primary
- Auth. response string:
- ☐ Response is positive authentication
- Force read of at least 1 characters of target response
- On match action: Disconnect

Identificación de secuencia de login

Gracias a esta funcionalidad podréis hacer pruebas en los momentos en los que queráis.

Y ahora pasamos a lo que nos interesa, localizar la clave de un LDAP. Para ello tendremos que seleccionar el tipo de ataque a "Custom". Antes de entrar en faena, debéis configurar si la conexión es de tipo Telnet, es decir, que con un simple Telnet podríais interactuar con el servidor. Si esto es así, marcad "Use telnet negotiation", en caso de que la conexión no sea comprensible humanamente mediante Telnet, dejadlo sin marcar.

Si queréis limitar la cantidad de pruebas a realizar, podéis marcar en "Try to stay connected for" indicando la cantidad o "Unlimited" si no queréis que pare.

Ahora pasemos a definir nuestros parámetros pulsando el botón "Define sequence". La cantidad de parámetros de que disponéis es extensa, debido a ello os abrirá una nueva ventana donde podréis configurar cualquier parámetro que se os ocurra.

Una de las primeras opciones de que disponemos es "No UserID". Esto se utiliza cuando el servidor sólo pide clave. La siguiente opción es "Use pre-auth", que podéis emplear cuando antes de la autenticación el servidor solicita algún tipo de dato de parte del cliente (por ejemplo, cuando el servidor le pregunta al cliente qué versión del protocolo quiere utilizar). Si seleccionáis esta opción, os aparece una sección de "Pre-authentication sequence" para indicar qué datos debe esperar el Brutus a recibir y con qué datos debe responder.

Y, como dije antes, hasta aquí puedo leer... en esta entrega. La que viene, más :-)

En la próxima entrega:
Descubriendo la clave de un LDAP... o de lo que se tercie II

Andrés Méndez Barco
Manuel Baleriola Moguel<

Virus y RFID

¿Podrían utilizarse las etiquetas RFID como medio de propagación de un virus?

En el anterior artículo introdujimos al lector en las similitudes de cómputo y almacenamiento existentes entre las etiquetas RFID y los humanos. En esta ocasión nos centraremos en los datos almacenados en las etiquetas y el posible daño que pudieran ocasionar los mismos.



Sistemas RFID

La tecnología RFID es una de las tecnologías más prometedoras dentro de la computación ubicua. Un uso extendido de esta tecnología podría provocar una mejora significativa de los procesos de identificación (ej. cadena de suministro). Sin embargo, no todo son ventajas y existen importantes riesgos de seguridad asociados a esta nueva o no tan nueva tecnología.

Los sistemas RFID están formados por tres componentes principales. Las etiquetas son interrogadas por los lectores con el objetivo de obtener la información almacenada en las mismas. A continuación los lectores se comunican con las bases de datos a fin de obtener información adicional asociada con el ítem que esta etiquetado. Habitualmente es asumido que el canal de comunicación entre los lectores y las bases de datos es seguro. Por otro lado el canal de comunicación entre las etiquetas y los lectores no es seguro. Incrementar la seguridad de esta canal de comunicación (backward/forward channel) ha sido el objeto de un gran número de investigaciones.

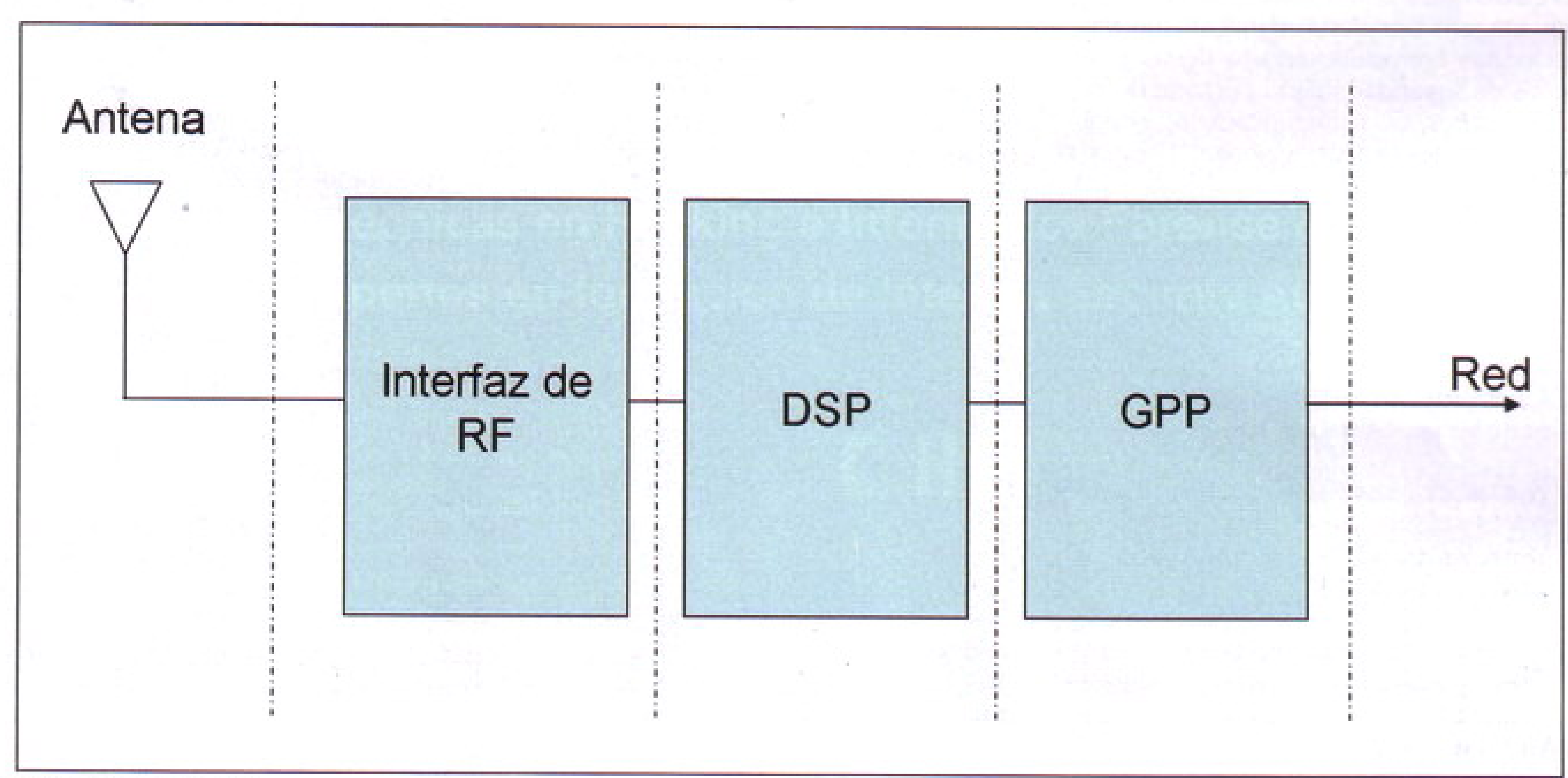
Virus en las etiquetas RFID

En este artículo nos centramos en un problema distinto, en concreto vamos a estudiar las vulnerabilidades de seguridad asociadas a los datos que obtenemos de las etiquetas. Recientemente se esta cuestionando la posibilidad de utilizar las etiquetas RFID para la propagación de virus. Imagínese la siguiente situación hipotética:

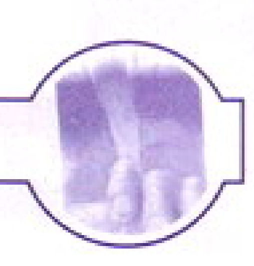
Supóngase que introduce en el sistema una etiqueta RFID en la cual están almacenados datos maliciosos los cuales permitirán explotar alguna vulnerabilidad de los lectores. Cuando esta etiqueta sea leída por el lector, se utilizará este agujero de seguridad provocando por ejemplo la ejecución de un determinado comando. Este comando podría hacer que se reconfigurara el lector para que este copiara los datos maliciosos en todos las etiquetas que escaneará en un futuro. Esto provocaría una propagación de los datos maliciosos en un gran número de etiquetas. A su vez, cuando una de las etiquetas infectadas fuera escaneada por otro lector, este sería infectado provocado una propagación más rápida de la infección.

Lo anterior es sólo un ejemplo de los que podría ocurrir si se utilizase las etiquetas RFID para la propagación de virus. Una vez leído este ejemplo el lector no debe tener la tentación de caer en el alarmismo. Hasta la fecha no existe ningún caso conocido de virus que tengan como objetivo la tecnología RFID, pero ciertas características de los sistemas RFID podrían ser utilizadas para explotar vulnerabilidades en el sistema y en sus bases de datos. La vulnerabilidad real asociada con el uso de los datos almacenados en las etiquetas subyace en como estos datos son usados y como estos datos son "tratados" antes de ser usados. Bases de datos pobremente diseñadas son vulnerables independientemente de la procedencia de los datos. Los datos no son sólo usados en los lectores, los cuales realizan únicamente un uso muy limitado de los mismos, sino que también son utilizados en los sistemas de información. Los sistemas de información son el objetivo de un gran número de virus. Las vulnerabilidades de seguridad debido a una pobre arquitectura de software o de implementación son totalmente diferentes de las vulnerabilidades de seguridad inherentes que podemos encontrar en el uso de los datos. Por ejemplo, el uso de un identificador simple como puntero en la base de datos no tiene vulnerabilidades de seguridad inherentes asociadas a su uso, sin embargo una pobre implementación de la petición SQL sería una vulnerabilidad de seguridad asociada a su implementación.

Los datos obtenidos de las etiquetas RFID no deben ser considerados seguros y no pueden ofrecernos ninguna confianza. Como consecuencia de esto, todos los datos deben ser analizados cuidadosamente a fin de de evitar posibles daños en el sistema. En este artículo nos centraremos en dos ataques en concreto. Co-



Arquitectura de un lector RFID



SI EL DESBORDAMIENTO DEL BUFFER SE PRODUCE CON UN PROGRAMA QUE TIENE PRIVILEGIOS DE ADMINISTRADOR, EL ATACANTE HEREDARÁ ESTOS PRIVILEGIOS

buffer ya que no fue comprobado el tamaño de los datos que iban a ser escritos en la "cadena2". (ver **Listado 1**)

Utilización del desbordamiento de buffer
Un desbordamiento de buffer provocará que la aplicación que hace uso de ese buffer deje de funcionar, perpetrándose un ataque de denegación de servicio. Sin embargo, los objetivos de la mayoría de estos ataques son muchos más ambiciosos. El objetivo del atacante es ejecutar un fragmento de código mediante el cual

>>> Listado 2

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

void subrutina(char *cadenain)
{
      char cadenaout[5];
      strcpy(cadenaout,cadenain);
      printf("Cadena copiada %s",cadenaout);
}

int main(int argc, char *argv[])
{
   subrutina(argv[1]);
};
```

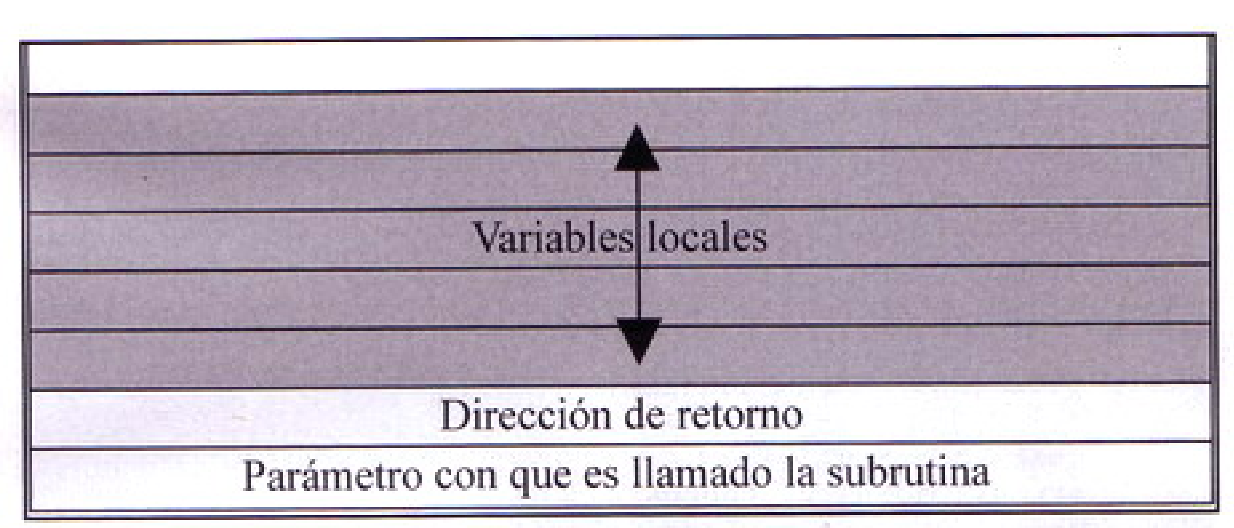
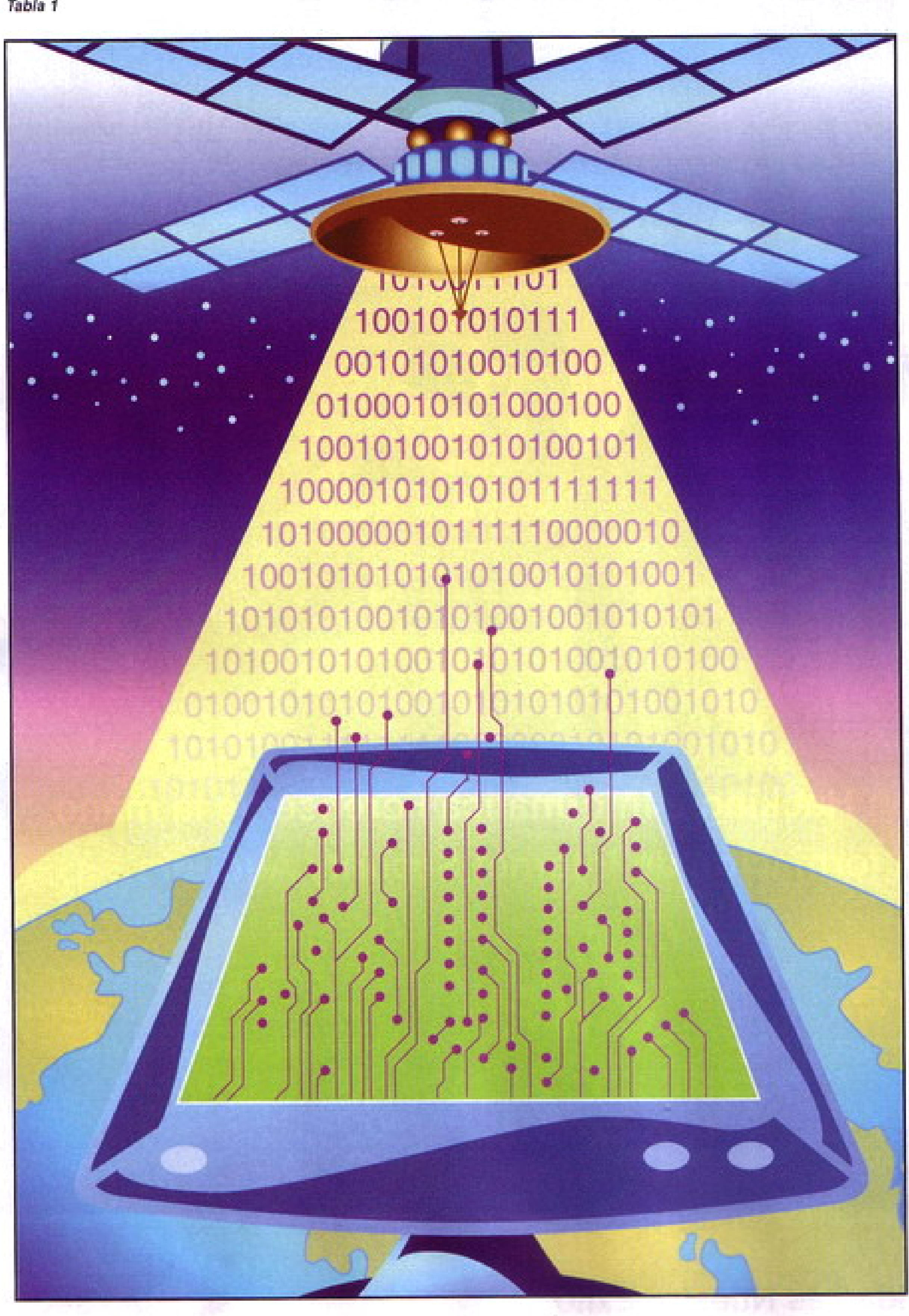


Tabla 1



podrá hacer casi todo lo que desee dependiendo de los privilegios con los que se ejecute. Si el desbordamiento del buffer se produce con un programa que tiene privilegios de administrador, el atacante heredará estos privilegios pudiendo hacer todo lo que desee. Sin embargo, si inicialmente el atacante no tiene privilegios de administrador, el ataque de desbordamiento de buffer podría utilizarse para realizar una escalada de privilegios, obteniéndose de nuevo privilegios de administrador.

Habitualmente los programas están organizados en subrutinas. En términos generales una subrutina es un "pequeño programa" que realiza una tarea. Siempre tendremos un programa principal que hace llamadas a subrutinas. Una vez la subrutina termina de ejecutarse (realiza su tarea) esta devuelve el control al programa principal.

TANTO SI NUESTRO OBJETIVO ES EL LECTOR COMO LA BASE DE DATOS, LA VIABILIDAD DE ESTE TIPO DE ATAQUES ESTARÁ MUY CONDICIONADA A LA CANTIDAD DE INFORMACIÓN QUE PUEDA SER ALMACENADA

Las subrutinas tienen que almacenar elementos de información para realizar su trabajo. Esta información se almacena en una zona de memoria denominada pila (stack). Adicionalmente en esta zona de memoria se almacena la dirección de retorno para cuando la subrutina termine su tarea.

Para facilitar su compresión al lector veremos un ejemplo: (ver **Listado 2**)

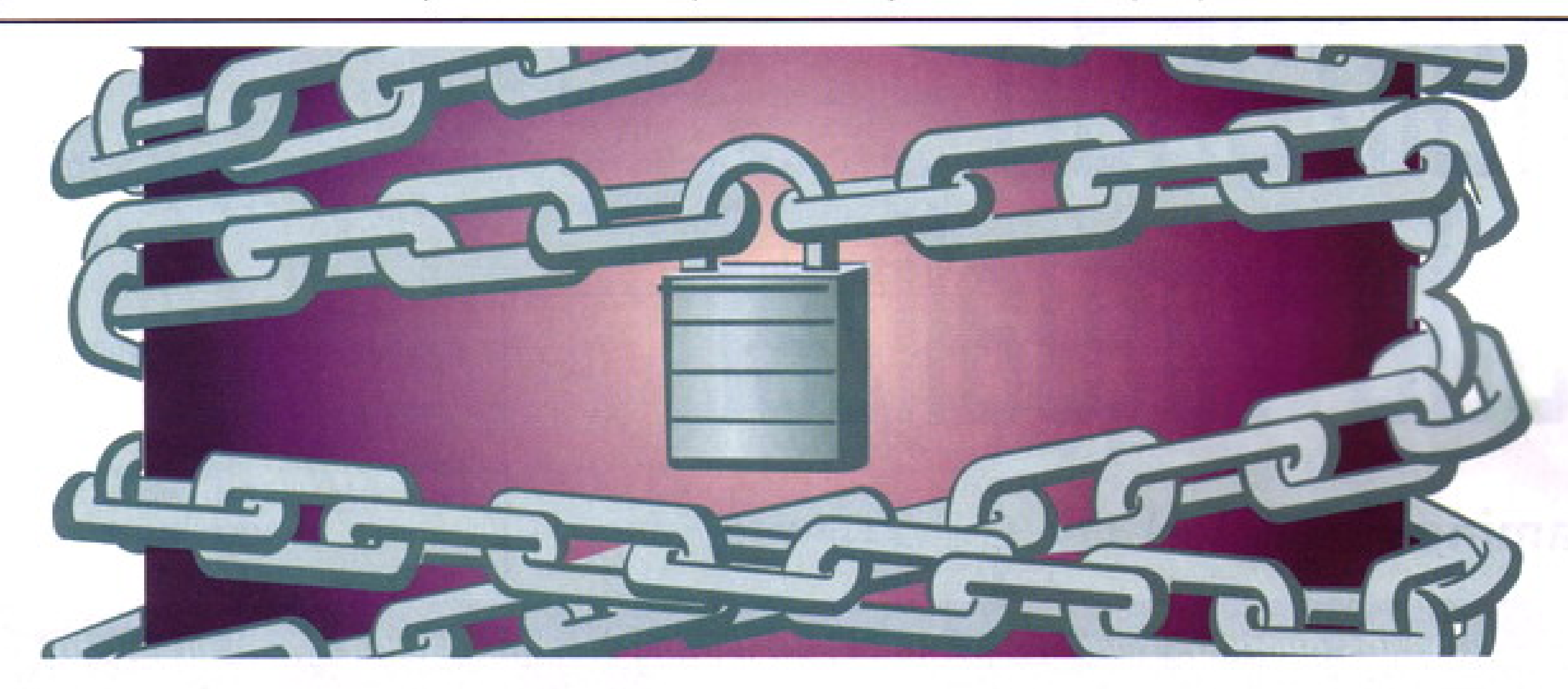
Mostramos a continuación la información que será guardada en la pila: (ver **Tabla 1**)

Como vemos en la figura anterior las subrutinas almacenan datos temporales en la pila. Cada vez que se hace una llamada a una subrutina, la memoria requerida es alojada en una zona de la pila denominada trama de pila (stack frame). En este espacio de memoria se almacenan todos los buffer necesarios así como la dirección de retorno de la subrutina. Cuando la subrutina termina esta salta a la dirección de retorno almacenada y borra la trama de pila utilizada.



>>> Enlaces

RFID y virus. http://www.rfidvirus.org/
Study Says Chips in ID Tags Are Vulnerables to Virases
http://www.nytimes.com/2006/03/15/technology/15tag.html?ei=5090&en=24f421ff24864376&ex=1300078800&partner=rssuserland&emc=rss&pagewanted=print
CERT Coordination Center Vulnerability Database http://www.kb.cert.org/vuls/
RFID y desbordamiento de buffer: http://www.wired.com/politics/security/news/2007/08/epassport



Todo lo anterior funciona correctamente hasta que un desbordamiento de buffer sucede. Si un usuario en el anterior programa llama a la función subrutina con un argumento de longitud N superior a 5 caracteres, los (N-5) caracteres extras sobrescribirán la zona de memoria adyacente en la trama de pila, sobrescribiendo posiblemente otros buffers así como la dirección de retorno. Bajo estas circunstancias la dirección de retorno será sobrescrita con lo que la subrutina no devolverá el control al programa principal. Si los N caracteres han sido cuidadosamente seleccionados por el atacante, el atacante puede conseguir que la dirección de retorno sea una zona de memoria donde tiene almacenado el código que desea ejecutar.

Resumiendo, un atacante debe realizar dos tareas para conseguir un fructuoso ataque de desbordamiento de buffer:

1.Cargar el código malicioso: esta tarea se realiza fácilmente escribiendo más caracteres en el buffer que los permitidos.

2.Ejecutar el código malicioso: esta tarea es más complicada, ya que la dirección de retorno debe ser la dirección donde esta almacenado el código malicioso. Controlar cual es la zona de memoria donde se almacenará el código es complicado y esta tarea se realiza habitualmente mediante prueba y error.

El tipo de desbordamiento de buffer que hemos visto es el más común (desbordamiento de buffer basado en pila) aunque existen otros tipos como por ejemplo el desbordamiento de buffer basado en la memoria "heap". Esperando que el lector haya comprendido el concepto de desbordamiento de buffer analizaremos sus implicaciones posibles en los sistemas RFID.

Lectores y desbordamiento de buffer

Los actuales lectores contienen dos procesadores:

1.Procesador encargado de los procesos de comunicación (DSP): modulación, demodulación, codificación y decodificación de la señal de radiofrecuencia, etc.

2.Procesador de propósito general (GP) encargado de la manipulación de datos, almacenamiento, peticiones, etc.

La existencia de estos dos procesadores dota de una mayor seguridad a los lectores. El DSP es la interfaz principal entre las etiquetas RFID y el sistema. Cualquier ataque de desbordamiento de buffer atacará primero al DSP. El software utilizado en un ordenador domestico es de uso común, facilitando su conocimiento para los atacantes. Sin embargo el software del DSP (firmware), es diferente en cada chip e incluso puede ser diferente entre versiones, lo cual dificulta la tarea del atacante.

El GP recibirá las entradas del DSP. Normalmente el GP realiza lectura de datos de una longitud fija, por lo que los ataques de desbordamiento de buffer solo tendrán efecto en el DSP. Si este último no tiene control sorbe el procesador principal ni la red, un ataque de desbordamiento de buffer no proporcionará ningún beneficio.

Bases de datos y desbordamiento de buffer

La protección que la base de datos ofrezca a los desbordamientos de buffer será inherente a la base de datos y no dependerá de los sistemas RFID. Por tanto, si la base de datos ha sido correctamente implementada debería ofrecer resistencia frente a este tipo de ataques.

Tanto si nuestro objetivo es el lector como la base de datos, la viabilidad de este tipo de ataques estará muy condicionada a la cantidad de información que pueda ser almacenada en las etiquetas. Desee cuenta el lector que existen un gran número de etiquetas (etiquetas de bajo coste) con fuertes limitaciones de almacenamiento, limitando así la aplicabilidad de este tipo de ataques.

En el siguiente artículo introduciremos al lector en los ataques de inyección de código y analizaremos su aplicabilidad a los sistemas RFID.

Pedro Peris-Lopez



CURSO de CRACK

Analizando Code Virtualizer

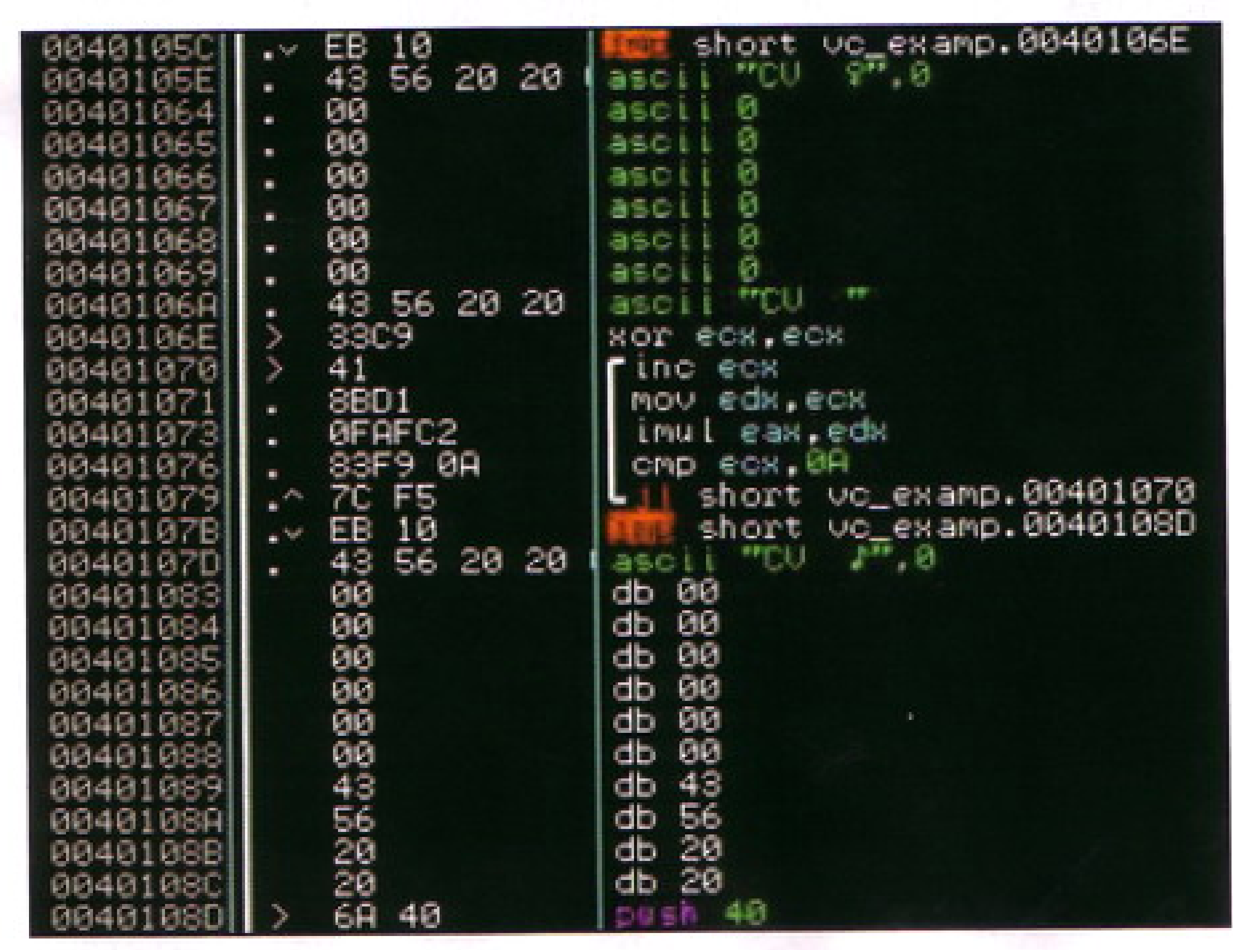
El camino de las VM

Hola a todos los queridos reversers... hoy les traigo nueva información de un producto interesante de la empresa Oreans. Se llama Code Virtualizer, ya un cracker muy conocido llamado scherzo lo ha analizado y repasaremos, relacionando y analizando los conocimientos brindados por él.

¿De qué se trata Code Virtualizer?

Como el nombre lo dice, es un programa para embeber una máquina virtual (VM) en nuestra aplicación, y que esta la proteja, complicando así el análisis.

Ya otros productos implementan estas técnicas, y hemos visto varios crackmes, y engines que hacen algo similar, con la única diferencia que este producto, está muchísimo más testeado y probado con diferentes compiladores.



ejemplo no virtualizado

Como sabemos, Oreans es la empresa que hace el producto Themida, un protector muy conocido también, el cuál implementa una VM y además muchas protecciones más.

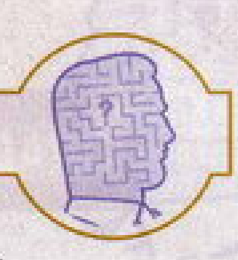
Estos protectores, reemplazan los opcodes x86 por opcodes generados únicamente para ESA aplicación protegida.

La VM que utiliza CodeVirtualizer, es denominada por Oreans, como Light VM, seguramente referido a la VM de Themida, que es mucho más compleja.

¿Con qué nos estamos enfrentando?

Cada VM generada posee unos 150 handlers, para poder manejar los códigos de operación generados.

Según lo analizado, las VM que genera Code Virtualizer, tiene una estructura para manejar los handlers. Esta estructura es denominada Handler_Information:



>>> Listado 1

```
006081DA    803E AC          CMP BYTE PTR DS:[ESI],0AC
006081DD    74 2A            JE SHORT 00608209
006081DF    66:813E 66AD     CMP WORD PTR DS:[ESI],0AD66
006081E4    74 23            JE SHORT 00608209
006081E6    803E AD          CMP BYTE PTR DS:[ESI],0AD
006081E9    0F85 A3020000    JNE 00608492
006081EF    817D 08 5401000  CMP DWORD PTR SS:[EBP+8],154
006081F6    0F84 96020000    JE 00608492
006081FC    817D 08 5601000  CMP DWORD PTR SS:[EBP+8],156
00608203    0F84 89020000    JE 00608492
```

WORD id: Un número o identificador que representa al handler.

DWORD start: Dirección de inicio del handler en el archivo de Code Virtualizer (CV de ahora en adelante)

DWORD end: Dirección del final del handler en el archivo de CV.

DWORD address: Dirección de la dirección de inicio del handler en el archivo protegido.

WORD order: Número aleatorio desde 0Eh a A4h que va indicar el lugar en donde está el handler en el archivo protegido.

Cada handler tiene su estructura, vemos una estructura de ejemplo:

```
id = 0000h;
start =006035F0h;
end = 006035F8h
```

Obviamente, existe un handler principal, que es bastante mas grande que el handler 0000h. Tiene algunas características especiales como por ejemplo 3 DWORDS que valen 11111111.

Ciertamente por cada aplicación protegida, esos DWORDS son únicos.

El primer DWORD es la dirección de la séptima linea del handler main, en el archivo protegido. El segundo, es la imagen base de la VM. El último DWORD es el número total de handlers utilizados en ESA VM.

Quizás muchos piensen que es muy dificultoso el tema de hacer que los códigos de operación sean diferentes por aplicación protegida, pero en realidad explicaré un poco como funciona este proceso.

```
section .code base 0000000h code

        XOR    ECX, ECX

@label1:
        INC    ECX

        MOV    EDX, ECX

        IMUL   EAX, EDX

        CMP    ECX, 10

        JL     @label1
        PUSH   00040108dh

        RET
```

code desensamblado por CV

Address	Hex dump	Disassembly
006035F0	AC	lods byte ptr ds:[esi]
006035F1	0FB6C0	movzx eax,al
006035F4	8D0487	lea eax,dword ptr ds:[edi+eax*4]
006035F7	50	push eax

handler0000

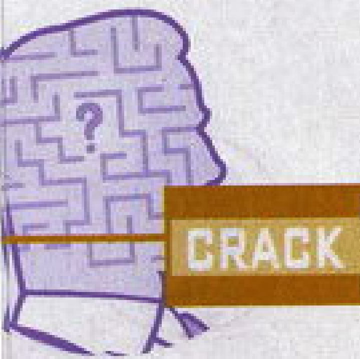
Lo primero que hace CV es crear el main handler, los demás 150 handlers son escritos en base a la información generada en el main handler, más específicamente por el campo Handler_Information.order.

Como mencioné antes desde 1E a A4, es el orden de la generación de los handlers. En la generación aleatoria de este orden de handlers, es lo que hace que cada VM y códigos de operación varíen también, en cuanto a significado.

Ahora veremos cómo CV genera el handler 0000h, y luego lo hace con cada uno de los demás handlers. En este código de CV podemos verlo: (ver Listado 1)

Los CMP son lods y obviamente, si hemos seguido los números anteriores en donde analizábamos las VM's y los generadores, sabemos que esta instrucción en el contexto de VM's, es utilizada para cargar los códigos de operación.

Los desarrolladores de Oreans, insertaron algunas instrucciones basuras para incrementar la seguridad.



sub eax,ebx	sub eax,Random1	sub eax,Random2	sub ebx,eax
add eax,ebx	add eax,Random1	add eax,Random2	add ebx,eax
xor eax,ebx	xor eax,Random1	xor eax,Random2	xor ebx,eax

Tabla 1

OreansX2.instruction	Instrucción
00	LOAD
01	STORE
02	MOVE
03	IFJMP
04	EXTRN
05	UNDEF
06	IMULC
07	ADC
08	ADD
09	AND
0A	CMP
0B	OR
0C	SUB
0D	TEST
0E	XOR
0F	MOVZX
10	MOVZX_W
11	LEA
12	INC

Tabla 2

Específicamente aquí se cargan los códigos de operación 1, 2 ó 4. Los desarrolladores de Oreans utilizaron otra estructura denominada por scherzo como Special_Handler.

Podemos ver la definición de esta estructura aquí:

WORD Handler_Information.id: tiene que ver con la información de la estructura de main.

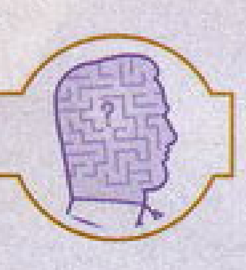
BYTE instruction3: significa que tipo de instrucción sera escrita como tercera instrucción.

BYTE instruction2: significa que tipo de instrucción sera escrita como la segunda instrucción.

BYTE instruction1: significa que tipo de instrucción sera escrita como la primera instrucción.

BYTE instruction4: significa que tipo de instrucción sera escrita como la cuarta instrucción.

DWORD Random1: número aleatorio que será parte de la instrucción 2.



OreansX2.instruction	Instrucción
13	RCL
14	RCR
15	ROL
16	ROR
17	SAL
18	SAR
19	SHL
1A	SHR
1B	DEC
1V	NOP
1D	MOVSX
1E	MOVSX_W
1F	CLC
20	CLD
21	CLI
22	CMC
23	STC
24	STD
25	STI
26	HLT

Tabla 3

DWORD Random2: número aleatorio que será parte de la instrucción 3.

Entonces, podemos ver probando, las posibilidades, en esta tabla de instrucciones: (ver Tabla 1)

Estas son las posibles, de ahí, los formatos pueden ser byte, word o dword, entonces se utilizarán los registros ax, bx, al, bl.

El siguiente paso para asegurar los handlers, es la mutación de ellos. A veces no son mutados, otras veces sí.

Esto sucede utilizando una función en la dll Oreansf1.dll llamada Oreansf1.F4. La mutación y ofuscación del código está directamente relacionada con la opción de complejidad del código mutado, que se encuentra en la GUI de la aplicación principal.

Esta complejidad no cambia la posibilidad de un ataque a CV. Lo cuál, no es algo vital para la seguridad de la aplicación.

El último paso y para finalizar... el código de cada handler mutado y generado es mezclado entre sí, para generar un único código ofuscado y complejo, prácticamente imposible de analizar.

Desarmando y armando de nuevo

Todo parece estar muy oscuro, pero no es así, podemos verlo simplemente compilando y probando los ejemplos que vienen en el paquete del software.

La función Oreansf1.F1 desensambla el archivo original y observaremos algo curioso. Todos los programas en donde se utilizan macros, poseen identificadores en forma de strings, especiales que le "dicen" al producto donde virtualizar o proteger.

Es el caso de CV también, pero, pero no utiliza ensamblador, sino que utilizan funciones nativas de Delphi, el lenguaje original utilizado por Oreans para desarrollar su producto.

Específicamente la función OreansX2dllR.F1 exportada por la dll, OreansX2dllR.dll se en-

```
XOR   byte ptr [ESP+000000008h *EDI + 012345678h], 18
      MOVE ADDR, DWORD PTR [F0000028h]   - 02 00 00 80 0E 00 00 00 28 00 00 F0 00 00
      SHL   ADDR, 3                      - 19 00 00 00 02 00 00 00 03 00 00 00 00 00
      ADD   ADDR, DWORD PTR [F0000038h]  - 08 00 00 80 0E 00 00 00 38 00 00 F0 00 00
      ADD   ADDR, 12345678h              - 08 00 00 00 03 00 00 00 78 56 34 12 00 00
      LOAD  BYTE PTR [ADDR]              - 00 00 00 00 04 00 00 00 00 00 00 00 00 00
      LOAD  BYTE 18                      - 00 00 00 00 20 00 00 00 12 00 00 00 00 00
      XOR   BYTE                         - 0E 00 00 00 18 00 00 00 00 00 00 00 00 00
      STORE FLAGS                        - 01 00 00 00 1E 00 00 00 00 00 00 00 00 00
      MOVE ADDR, DWORD PTR [F0000028h]   - 02 00 00 80 0E 00 00 00 28 00 00 F0 00 00
      SHL   ADDR, 3                      - 19 00 00 00 02 00 00 00 03 00 00 00 00 00
      ADD   ADDR, DWORD PTR [F0000038h]  - 08 00 00 80 0E 00 00 00 38 00 00 F0 00 00
      ADD   ADDR, 12345678h              - 08 00 00 00 03 00 00 00 78 56 34 12 00 00
      ADD   ADDR, 00000002h              - 08 00 00 00 03 00 00 00 00 00 00 20 00 00
      STORE BYTE PTR [ADDR]              - 01 00 00 00 04 00 00 00 00 00 00 00 00 00
```

sintaxis de CV

carga de ensamblar, lo desensamblado y modificado por el programa.

Genera una de las estructuras más importantes denominada OreansX2. Aquí podemos ver la estructura:

DWORD instruction: tipo de instrucción seguida por la sintaxis de CV.

DWORD sux: sufijo para la instrucción.

DWORD data1: datos para la instrucción.

DWORD data2: datos para la instrucción.

WORD unknown: su uso es desconocido.
Las posibles combinaciones creadas, junto a sus identificadores, son: (ver Tabla 2)

Esa es la primera parte, y la segunda parte de la tabla, la podemos ver aquí: (ver Tabla 3)

Como podemos observar, las instrucciones son generadas con una estructura y pensamiento lógico, ya que las instrucciones básicas como XOR, ADD se denominan así, mientras que instrucciones como MOV, se denominan MOVE, STORE, entre otras.

Luego siguen las otras tablas precalculadas, de sufijos y estructuras para armar estas instrucciones.

Generando y escribiendo Códigos de operación virtuales

Seguido a todo este proceso que estamos describiendo, continúa la generación de algo que Scherzo llamo Pre Handlers. El tamaño que tiene esta estructura es de 28h.

TODO PARECE ESTAR MUY OSCURO, PERO NO ES ASÍ, PODEMOS VERLO SIMPLEMENTE COMPILANDO Y PROBANDO LOS EJEMPLOS QUE VIENEN EN EL PAQUETE DEL SOFTWARE

Podemos ver esta definición:

DWORD counter: contador que es incremebtado por 0Eh para cada estructura Pre Handler.

DWORD real_opcode_mark: es la dirección de los códigos de operación originales en una zona de memoria que está reservada. Esto es solamente aplicable al resto de las instrucciones de CV del bloque de instrucciones que representan los códigos de operación originales.

DWORD unknown1: uso desconocido.

DWORD counter_0E: contador para la estructura Pre Handler, incrementado 0Eh.

BOOL is_special: toma un valor verdadero, si el código de operación original es algún tipo de llamado (CALL) o salto (condicional o incondicional). En este caso, una estructura especial, será generada para estas instrucciones.

BYTE instruction: lo mismo que OreansX2.instruction.

DWORD sux: lo mismo que OreansX2.sux.

DWORD data1: lo mismo que OreansX2.data1.

DWORD data2: lo mismo que OreansX2.data2.

WORD unknown2: lo mismo que OreansX2.unknown.

Existen 7 bytes desconocidos.

BOOL is_relative_address: este campo es verdadero si la instrucción tiene una dirección relativa.

Conclusión

Bien amigos, estamos investigando, analizando, y tomando como dije al principio del artículo, el conocimiento de nuestro amigo Scherzo.

Code Virtualizer, es un producto muy interesante, y seguiremos analizándolo en el próximo número, hay más sorpresas. :)

Espero que les haya gustado.

Nos vemos en el próximo número.

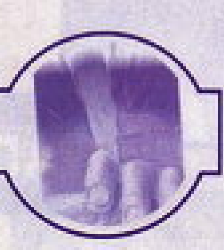
SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com



servidores de replicación

Asegurando la información de nuestras bases de datos

A día de hoy, prácticamente cualquier sistema automatizado de tratamiento de información pasa, de una u otra forma, por una base de datos. Desde las pequeñas bases de datos que todos manejamos, hasta las inmensas amalgamas de información de las bases de datos empresariales o gubernamentales, todas ellas se rigen por los mismos principios básicos. Y, seguramente, el más importante de dichos principios sea conservar la integridad de los datos contenidos en el sistema.





Saludos una vez más, apreciado lector. Como comentaba en la introducción del presente artículo, actualmente vivimos todos nosotros rodeados de bases de datos. Y, para bien o para mal, nuestra información personal se encuentra desperdigada por infinidad de bases de datos: desde las legítimas e imprescindibles bases de datos estatales sobre la población (como el padrón), hasta las abiertamente ilegales y molestas de los spammers, pasando por las -en ocasiones- dudosamente legales y omnipresentes de las grandes empresas.

No es extraño que, en el ámbito particular, una persona posea una base de datos con información de, por ejemplo, su colección de libros o películas (yo, por ejemplo, tengo una). Entrando ya en el terreno profesional, y para aquellos cuya formación u orientación profesional se dirija a la informática, creo que todos hemos tenido que lidiar con diferentes sistemas gestores de bases de datos. Y, peor aún, con las bases de datos contenidas en ellos, que no siempre están a la altura del nombre que hay tras ellas. Me viene a la cabeza cierta compañía aeronáutica europea, de cuya base de datos prefiero no acordarme...

Los datos, siempre los datos

Como su propio nombre indica, en una base de datos lo más importante son los datos. Parece una perogrullada, lo sé, pero conviene recordarlo para no caer en el típico error de perderse en la interfaz de usuario y olvidar lo que realmente importa. Que luego nos puede salir Access y pasa lo que pasa...

Así, todo sistema gestor de bases de datos (SGBD) debe cumplir una serie de propiedades que se definen para garantizar la integridad de los datos contenidos en ellos. Una de dichas propiedades, y seguramente la más importante de todas ellas, es la famosa integridad referencial, encargada de garantizar que una entidad siempre se relaciona con otras entidades de una forma válida, según el modelo entidad/relación que define a la base de datos en cuestión.

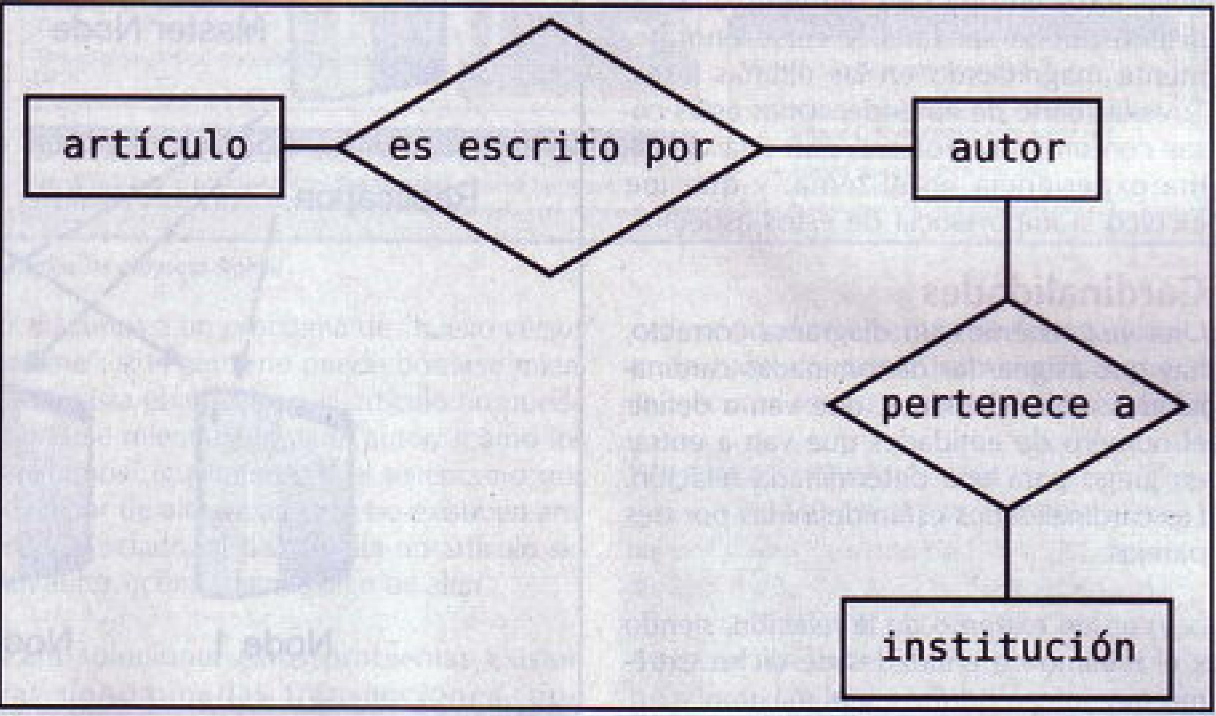
Entre los errores más típicos que rompen la integridad referencial de una base de datos, podemos encontrar: datos incorrectos o de un tipo diferente al que deberían contener, datos repetidos y/o incongruentes, datos perdidos, relaciones que no cumplen las condiciones de cardinalidad mínima...

Modelo entidad/relación

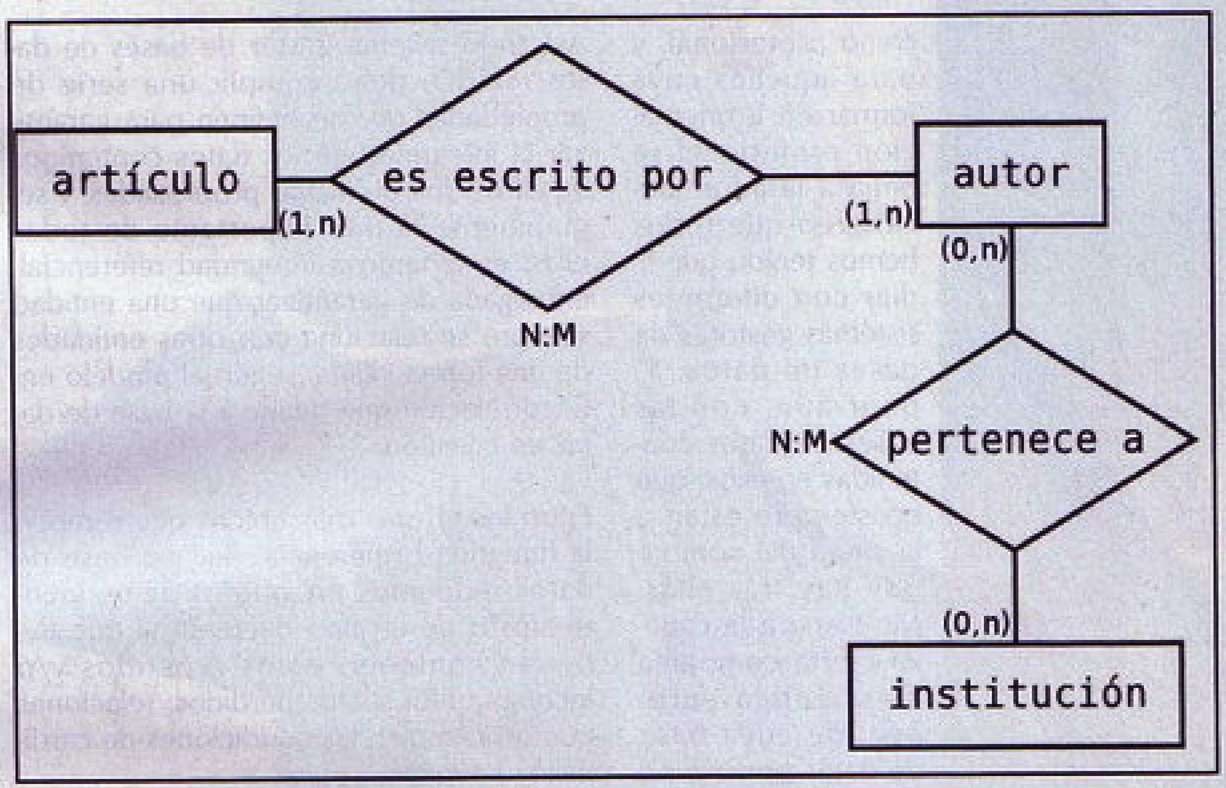
Cuando queremos diseñar una base de datos, y si pretendemos hacerlo de la forma correcta, se hace necesario seguir una serie de pasos. El primero de ellos es decidir qué entidades van a intervenir en nuestro sistema, y cuáles van a ser las relaciones que las permitan interaccionar. A este paso se le conoce como generación del diccionario de datos.

Tras la generación del diccionario, el segundo paso es diseñar el modelo entidad/relación del sistema.

En la imagen adjunta veréis un ejemplo muy simple en el que intervienen las entidades "artículo", "autor" e "institución"; así como las relaciones "es escrito por" y "pertenece a".



Ejemplo de modelo entidad-relación



Cardinalidades

No creo necesario entrar en demasiados detalles sobre el diseño de modelos de entidad/relación, más que nada porque podríamos estar varios meses tranquilamente hablando del tema, y además creo que este sencillo ejemplo resulta lo suficientemente intuitivo. Del diagrama podemos deducir lo siguiente:

Un artículo es escrito por un autor.
Un autor escribe artículos.
Un autor pertenece a una institución
Una institución tiene autores.

En este caso puede parecer trivial, pero la correcta generación de un diagrama en el que intervengan decenas o cientos de entidades y relaciones, puede llevar una gran cantidad de trabajo. Además, cualquier error en una fase tan temprana del diseño puede ser fatal, y verse enormemente magnificado en las últimas fases. Tuve la suerte de aprender todas estas cosas con un gran profesor, con una vastísima experiencia en el tema, y que me inculcó la importancia de estos aspectos.

Cardinalidades

Una vez tenemos un diagrama correcto, hay que asignar las denominadas cardinalidades a las relaciones, que van a definir el número de entidades que van a entrar en juego para una determinada relación. Las cardinalidades están definidas por tres parejas:

(x,y) en un extremo de la relación, siendo x el mínimo de entidades de dicho extremo que intervendrán, e y el máximo.

TODO SISTEMA GESTOR DE BASES DE DATOS DEBE CUMPLIR UNA SERIE DE PROPIEDADES QUE SE DEFINEN PARA GARANTIZAR LA INTEGRIDAD DE LOS DATOS CONTENIDOS EN ELLOS

(i,j) en el otro extremo de la relación, con las mismas connotaciones.

Y:J en la relación, que definirá la cardinalidad general de la relación.

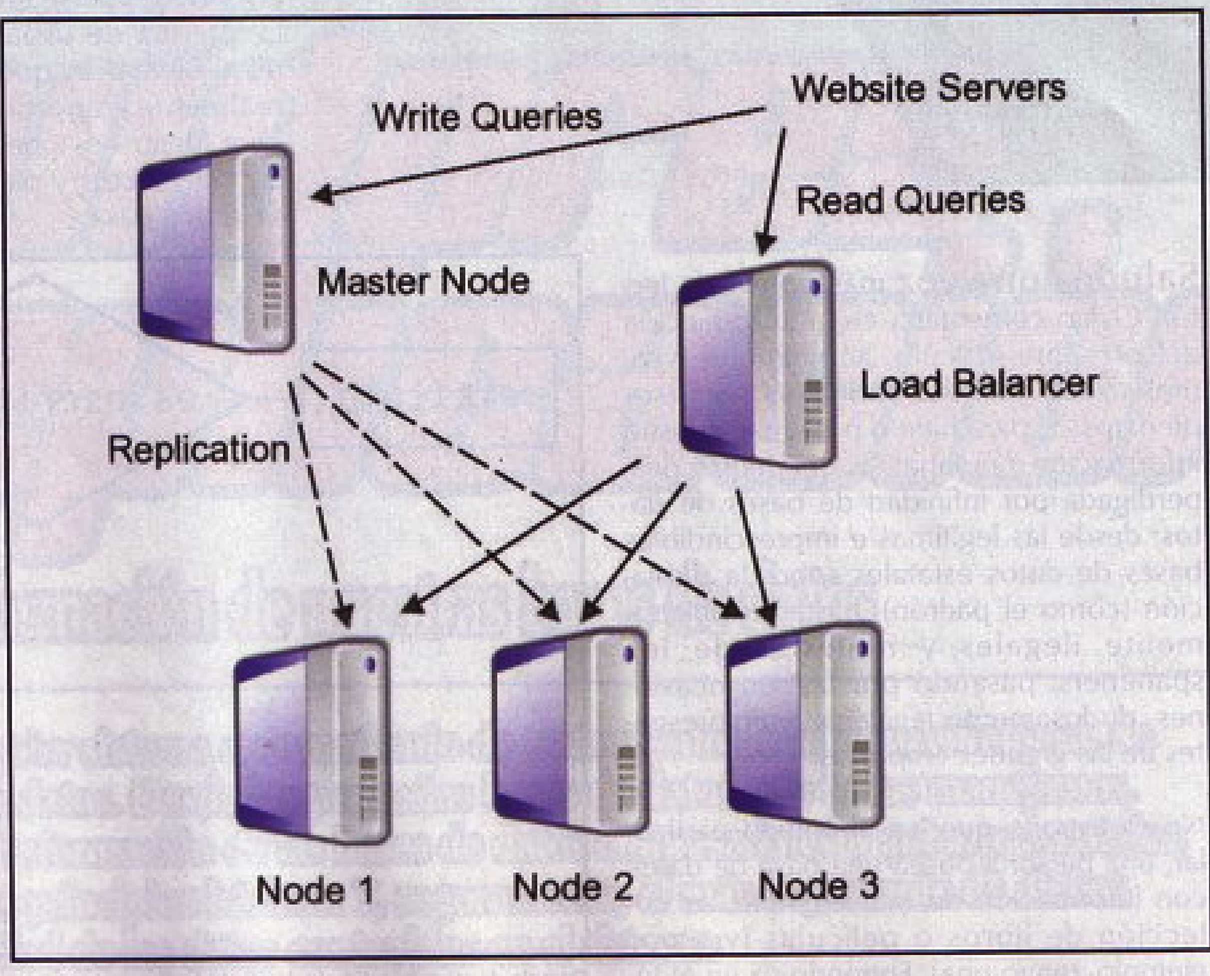
Además, hay que tener en cuenta las siguientes consideraciones:

La cardinalidad mínima sólo puede ser 0 ó 1. En caso de ser más de 1, se considerará 1 y se especificará en una anotación el dato concreto, que se tendrá en cuenta en fases posteriores del diseño.

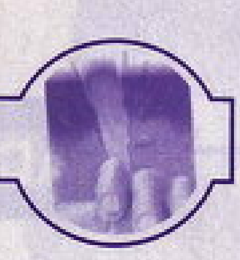
La cardinalidad máxima sólo puede ser 1 ó n. En caso de ser un número concreto, se seguirá el mismo proceso de realizar una anotación con el dato, que se considerará más adelante.

La cardinalidad de la relación, dado que se calcula con las cardinalidades máximas de las entidades, sólo podrá ser "1:1" (relación "de uno a uno"), "1:N" (relación "de uno a muchos") o "N:M" (relación de muchos a muchos).

Veamos cómo se aplicaría a la relación "artículo - es escrito por - autor". En primer lugar definiremos la cardinalidad de la entidad "artículo" de la siguiente forma: un autor, para ser considerado como tal, deberá haber escrito como mínimo un artículo, y como máximo muchos; por lo que tendrá cardinalidad "(1,n)". Para la entidad "autor" haremos la misma consideración: un artículo, para poder existir, debe haber sido escrito como mínimo por un autor, y como máximo por muchos (he visto publicaciones con listas de



Arquitectura de un sistema replicado



autores que daban miedo...); por lo que la cardinalidad será de "(1,n)". Así, la cardinalidad de la relación será "N:M", o de muchos a muchos. Las implicaciones de esta cardinalidad se dejarán notar en el paso al modelo relacional del sistema, aunque nosotros no llegaremos tan lejos para ilustrar este ejemplo.

Para el caso de la relación "autor - pertenece a - institución" haremos lo mismo. Un autor puede pertenecer o no a una institución, y además puede pertenecer a varias, por lo que tenemos una cardinalidad "(0,n)". Por su parte, una institución podrá no tener autores, o tener muchos, por lo que la cardinalidad también será de "(0,n)". Así, la relación también tendrá una cardinalidad "N:M".

En la imagen adjunta podemos ver el modelo con sus cardinalidades ya asignadas.

Integridad referencial

Ahora, y teniendo presente el esquema anterior, analizaremos determinadas situaciones que suponen una violación de la integridad referencial de la base de datos:

La base de datos únicamente contiene un autor. Dado que un autor no tiene por qué pertenecer a una institución, en esa relación no tendríamos ningún problema. Pero, dado que definimos que un autor debe tener asociado como mínimo un artículo, esta situación no cumpliría la integridad referencial.

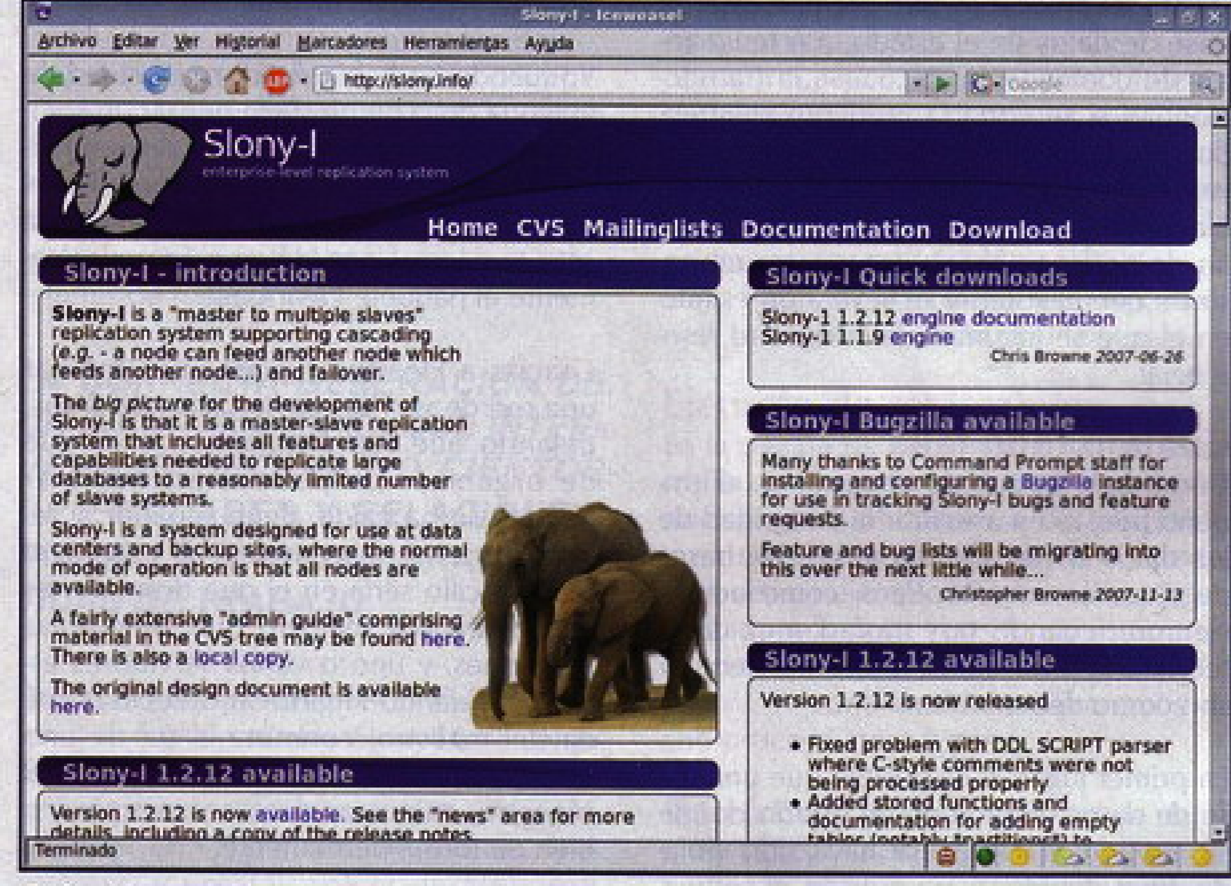
La base de datos únicamente contiene un artículo. Por el mismo motivo que en el ejemplo anterior, y dado que un artículo debe pertenecer como mínimo a un autor, de nuevo estaríamos en una situación ilegal desde el punto de vista de la integridad referencial.

La base de datos contiene un artículo y un autor, pero no están relacionados entre sí. Sería una combinación de los dos supuestos anteriores, por parte de ambas entidades.

Por supuesto, y una vez hemos definido nuestra base de datos correctamente en el sistema gestor de bases de datos, estas situaciones no podrían darse, pues arrojarían errores o excepciones al tratar de inducirlas. Igualmente, si tenemos un único autor y un único artículo, ambos relacionados, el sistema no debería dejarnos borrar ninguno de los dos mientras exista el otro.



Página de Heartbeat en el proyecto Linux-HA



Página del proyecto Slony-I

Y llegamos a un problema de "huevo versus gallina": si el autor no puede borrarse mientras exista el artículo, y el artículo no puede borrarse mientras exista el autor, ¿como los borramos? Igualmente, si el sistema no nos deja dar de alta un autor si no existe un artículo asociado, ni dar de alta un artículo sin un autor, ¿cómo damos algo de alta?

Para solucionar estos problemas existen las denominadas transacciones, que podríamos definir como un conjunto de órdenes que se ejecutan de forma atómica en la base de datos. Esto significa que, o se ejecutan todas, o ninguna. Por ejemplo:

```
EMPIEZA TRANSACCIÓN
     DAR DE ALTA AUTOR "Ramiro" -> "escribe" -> "Linux mola"
     DAR DE ALTA ARTÍCULO "Linux mola" -> "es escrito por" -> "Ramiro"
EJECUTAR TRANSACCIÓN
```



Paquete de Slony-I en Debian

Dado que ambas instrucciones en conjunto sí cumplen la integridad referencial, la transacción también lo hace. ¿Y si la transacción arroja un error? Pues existe una zona de memoria denominada segmento de "rollback" que permite dejar la base de datos en el estado que tenía antes de comenzar a ejecutarse la transacción. ¿Y si se corta la corriente eléctrica durante la ejecución? Existen ficheros de registro con las operaciones que se efectúan sobre la base de datos, con el fin de poder revertirlas una a una en caso de que el sistema se lleve a un estado en el que se incumpla la integridad referencial.

Cuando todo falla

Como habréis podido comprobar, el empeño puesto en asegurar la integridad de los datos en un sistema gestor de bases de datos es enorme. Pero, como ocurre siempre, cuando nos trasladamos de la teoría a la práctica, las cosas no siempre son como deberían ser.

En primer lugar, sí es posible que una base de datos termine en un estado donde su integridad referencial haya sido violada, bien debido a un error en el software, a la laxitud en la implementación de las directivas ACID (Atomicity, Consistency, Isolation and Durability: Atomicidad, Consistencia, Aislamiento y Durabilidad) en un sistema transaccional, o por cualquier otro motivo.'

Por otro lado, y ya entrando en el terreno de servidores de bases de datos, nunca estamos libres de un hipotético fallo del software o del propio sistema operativo. Además, en un sistema con una carga de peticiones muy alta, podemos encontrarnos en la situación de que el servidor no sea capaz de atender el volumen de solicitudes entrante. Por tanto, la disponibilidad de una base de datos depende de otros factores externos, además de lo que pueda ocurrir con los datos contenidos en ella.

Y, cuando se habla de disponibilidad, la mayoría de la gente suele pensar en soluciones de clustering de alta disponibilidad o granjas de servidores. Uno de los proyectos más famosos con respecto a este tema es Linux-HA, y más concretamente el paquete Heartbeat.

Gracias a Heartbeat podríamos montar una red de servidores de bases de datos, dejando que sea él quien se encargue de organizar las peticiones, detectar cuándo se ha caído algún servidor, y reaccionar en consecuencia. El escenario más sencillo sería en el que disponemos de un servidor maestro que atiende las peticiones, y uno o varios servidores esclavos. Cuando Heartbeat detecta la caída del maestro, conmuta el rol de uno de los esclavos para que pase a ser el maestro, mientras éste se recupera o bien de forma permanente.

Pero, como venimos diciendo desde el comienzo del presente artículo, lo más importante en una base de datos son los propios datos contenidos en ésta. Así, si disponemos de una granja de servidores configurados en un entorno de alta disponibilidad, necesitaremos además asegurarnos de que contienen, en todo momento, exactamente los mismos datos, o de nada habrá servido que se detecte la caída del maestro y se conmute por un esclavo.

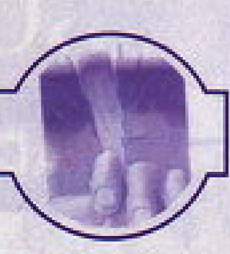
Y aquí es donde entra en juego la replicación de datos.

Replicación de datos

Bien sea por implementar un sistema de alta disponibilidad o por balancear la carga de las peticiones en una granja de servidores, necesitaremos que los datos de una base de datos estén sincronizados en todo momento, o por lo menos con la suficiente agilidad como para no ocasionar perjuicios en las consultas lanzadas por los sistemas o usuarios finales.

Así, debemos definir unas reglas por las cuales la información de la base de datos, que en el ámbito de la replicación se conoce con el término de "publicación", pueda ser transferida de un nodo que actúe como "publicador" a otro que actúe como "suscriptor". Dicha transferencia puede ser llevada a cabo por un tercer elemento, un servidor que actúe como "distribuidor remoto" de datos. En caso de no existir dicho nodo independiente, se considera que el nodo publicador es también distribuidor.

En primer lugar, hay que definir el sentido del tráfico de la replicación de los datos, pudiendo ser unidireccional o bidireccional. En el primer caso, únicamente el nodo maestro puede modificar los datos de las bases de datos, que más tarde propagará a todos sus suscriptores para que actúen como "copias de sólo lectura". Este caso suele darse cuando la base de datos es accedida para consulta únicamente (o casi), por ejemplo para ser puesta a disposición de Internet mediante una página web. En el segundo caso, la comunicación bidireccional permite que las modificaciones se realicen en el



>>> Listado 1

```
Join existing cluster: Checked
Server:                <Select the server containing the master database>
Database:              master
Cluster name:          pgbench
Local node:            10        Slave node 1
Admin node:            99 - Admin node

Join existing cluster: Checked
Server:                <Select the server containing the master database>
Database:              master
Cluster name:          pgbench
Local node:            20        Slave node 2
Admin node:            99 - Admin node
```

nodo maestro o en cualquiera de sus esclavos. Este sistema es más flexible, pero a costa de una mayor complejidad a la hora de sincronizar los datos. Además, en este último caso podríamos tener replicaciones desde los esclavos al maestro y después al resto de esclavos (en árbol) o directamente entre todos los nodos (en estrella).

Por otro lado, se debe definir el modo de actualización de los datos cuando ocurre un cambio, pudiendo ser síncrono o asíncrono. En el modo de replicación síncrono los datos son replicados en el mismo instante en que se introducen las modificaciones, mientras que en el asíncrono se realiza en unos determinados instantes de tiempo que vienen dados por la configuración propia del sistema. El primer modo proporciona una mayor disponibilidad de los datos, prácticamente en tiempo real, pero a costa de una mayor complejidad y un consumo de ancho de banda bastante elevado (dependiendo del volumen de modificaciones que soporte la base de datos). Normalmente, cuando una base de datos replicada es modificada con una alta frecuencia, suele utilizarse un sistema de replicación asíncrono, que además suele coincidir con las horas más bajas de utilización de la red y del sistema (típicamente por la noche).

La actualización de datos síncrona, a su vez, puede darse a nivel de aplicación o a nivel de subsistema de almacenamiento. En el primero de los casos, el sistema gestor de bases de datos será el encargado de replicar la información atendiendo a sus parámetros internos. Cuando el encargado de la tarea es el nivel de subsistema de almacenamiento, será el hardware el encargado de replicar los datos.

Software de replicación

Como podréis imaginar, hoy en día cualquier empresa o institución con una base de datos de un tamaño respetable, necesita disponer de un sistema de replicación para su gestor de bases de datos. Así, prácticamente cualquier sistema gestor de bases de datos medianamente serio dispone hoy en día de una o varias soluciones que permitan establecer soluciones de replicación.

LA CORRECTA GENERACIÓN DE UN DIAGRAMA EN EL QUE INTERVENGAN DECENAS O CIENTOS DE ENTIDADES Y RELACIONES, PUEDE LLEVAR UNA GRAN CANTIDAD DE TRABAJO

Por ejemplo, en PostgreSQL disponemos de los complementos Slony-I (así como de Slony-II) y PGcluster, en MySQL disponemos de la herramienta "MySQL cluster", en Oracle disponemos de "ShaRePlex", y en SQL Server de Microsoft disponemos de compatibilidad nativa para estas operaciones.

SQL Server es una solución de software privativo (y caro, además), por lo que su implantación queda reservada prácticamente a empresas con el suficiente presupuesto para adquirir las costosas licencias, y las suficientes ganas como para lidiar con servidores Windows. MySQL es, seguramente, uno de los sistemas gestores de bases de datos más utilizados en la actualidad, pero a la hora de trabajar con grandes bases de datos puede "atragantarse" un poquito (doy fe).

Personalmente, creo que para gestionar grandes bases de datos, y siempre que se opte por el software libre, la mejor opción es PostgreSQL. Además, es multiplataforma, por lo que perfectamente podemos disponer de varios servidores con diferentes sistemas operativos y replicando una misma base de datos gracias a Slony-I. Además, también podemos comnbinar la replicación de Slony-I con un sistema de alta disponibilidad, por ejemplo mediante Heartbeat.

Ejemplo de replicación

En la página de documentación de desarrollo del paquete pgAdmin (una herramienta multiplataforma de gestión y monitorización de PostgreSQL) podemos ver un ejemplo de cómo desplegar, en catorce sencillos pasos, un sistema de replicación mediante PostgreSQL y Slony-I. A continuación analizaremos dicho proceso, paso a paso.

1) Lo primero es crear las bases de datos para la replicación. Como mínimo deberán ser dos (un maestro y un esclavo), aunque en el ejemplo se crean tres bases de datos, una que actuará como maestro ("master") y dos que actuarán como esclavos ("slave1" y "slave2"). Es muy importante asegurarse de que el lenguaje PL/PgSQL está activado en todas y cada una de las bases de datos.

2) A continuación, debe crearse un esquema en la base de datos que actúa como maestro ("master"). En el ejemplo, el esquema es creado mediante la utilidad pgbench, que puede encontrarse en el directorio

>>> Listado 2

```
Table:                   public.accounts
ID:                      1
Index:                   accounts_pkey

Table:                   public.branches
ID:                      2
Index:                   branches_pkey

Table:                   public.history
ID:                      3
Index:                   history_pkey

Table:                   public.tellers
ID:                      4
Index:                   tellers_pkey
```

"contrib" de las fuentes de PostgreSQL.

```
> pgbench -i -U postgres master
```

3) Debe añadirse una clave principal a la tabla. Podéis hacerlo como queráis, aunque en el ejemplo se crea una clave principal mediante la combinación de tres columnas de la relación.

4) A continuación, debe volcarse en un fichero SQL el esquema (y únicamente el esquema) de la base de datos "master" para poder copiarlo en las bases de datos esclavas "slave1" y "slave2". Dado que la replicación únicamente actuará a nivel de datos, es necesario que el esquema de todas las bases de datos sea congruente antes de comenzar el proceso.

```
> pg_dump -s -U postgres mas-
ter > schema.sql
> psql -U postgres slave1 <
schema.sql
> psql -U postgres slave2 <
schema.sql
```

5) El siguiente paso requiere la creación de los ficheros de configuración para cada motor slon (en sistemas Linux, demonios del sistema). Un ejemplo minimalista de dicho fichero de configuración es el siguiente:

```
cluster_name='pgbench'
conn_info='host=127.0.0.1
port=5432 user=postgres dbna-
me=master'
```

En este caso el nodo es el propio sistema (localhost, 127.0.0.1) porque la prueba está montada en local, pero es perfectamente posible realizarla con varios sistemas en una red y configurar las direcciones IP pertinentes. Los demás parámetros de conexión son el puerto, el usuario del servicio (postgres es el que se crea por defecto en la configuración de PostgreSQL) y el nombre de la base de datos a replicar.

6) Este paso es exclusivo de sistemas Windows, y consiste en instalar el servicio de Slony-I:

```
> slon -regservice Slony-I
```

7) Es el momento de registrar cada motor Slon en el sistema. En sistemas Windows debemos ejecutar los siguientes comandos:

```
> slon -addengine Slony-I
<ruta_a_master.conf>
> slon -addengine Slony-I
<ruta_a_slave1.conf>
> slon -addengine Slony-I
<ruta_a_slave2.conf>
```

Donde cada comando deberá tener la ruta al fichero de configuración pertinente, que creamos en el quinto paso. En sistemas Linux, se deben arrancar los demonios de forma manual e independiente, pasándole la ruta al fichero de configuración mediante el parámetro "-f".

8) Ahora, crearemos un cluster de Slony-I en pgAdmin, en el nodo de replicación de la base de datos "master". Las opciones a utilizar serán las siguientes:

Join existing cluster: Unchecked		
Cluster name:	pgbench	
Local node:	1	Master node
Admin node:	99	Admin node

9) Repetiremos el paso anterior para cada una de las bases de datos esclavas. Las opciones para las dos bases de datos de nuestro ejemplo serán: (ver Listado 1)

10) El siguiente paso requiere crear las rutas desde el maestro a ambos esclavos, y desde cada uno de los esclavos al maestro. Para ello, usaremos la misma cadena de configuración que vimos en el fichero de configuración del motor Slon.

11) Ahora se debe crear un conjunto de replicación (Replication Set) en el maestro, con las siguientes opciones:

```
ID:                1
Comment:           pgbench set
```

12) Añadiremos a continuación las tablas al conjunto de replicación para conformar los datos de la suscripción. Utilizaremos las siguientes opciones: (ver Listado 2)

13) Con los datos de la suscripción, generaremos ahora una nueva suscripción para cada uno de los nodos esclavos, utilizando las siguientes opciones:

```
Origin:            1
Provider:          1 - Mas-
ter node
Receiver:          10 - Sla-
ve node 1

Origin:            1
Provider:          1 - Mas-
ter node
Receiver:          20 - Sla-
ve node 2
```

14) Por último, iniciaremos el servicio Slon (o el demonio en Linux):

```
> net start Slony-I
```

La replicación debería comenzar inmediatamente. Para comprobar su correcto funcionamiento, podemos lanzar sentencias de inserción o modificación contra la base de datos "master", de forma que veamos cómo dichos cambios se propagan a los dos nodos esclavos. Utilizar la herramienta de pruebas de carga pgbench puede facilitar el trabajo, al evitar el tedioso proceso de lanzar manualmente todas las consultas.

Finalizando

Como habéis podido comprobar, los actuales sistemas gestores de bases de datos son capaces de soportar una enorme cantidad de carga, así como de conformar complejos sistemas de trabajo distribuido cuando un único servidor es insuficiente. Y es que, debido a la importancia y magnitud de las actuales bases de datos, es absolutamente imprescindible la existencia de este tipo de sistemas, pues hay gran cantidad de situaciones en las que no podemos permitirnos que los datos estén inaccesibles, aunque sea durante un pequeño período de tiempo. ¡Nos leemos!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com



AÑO 9 (??? ¿YA?), NÚMERO 126

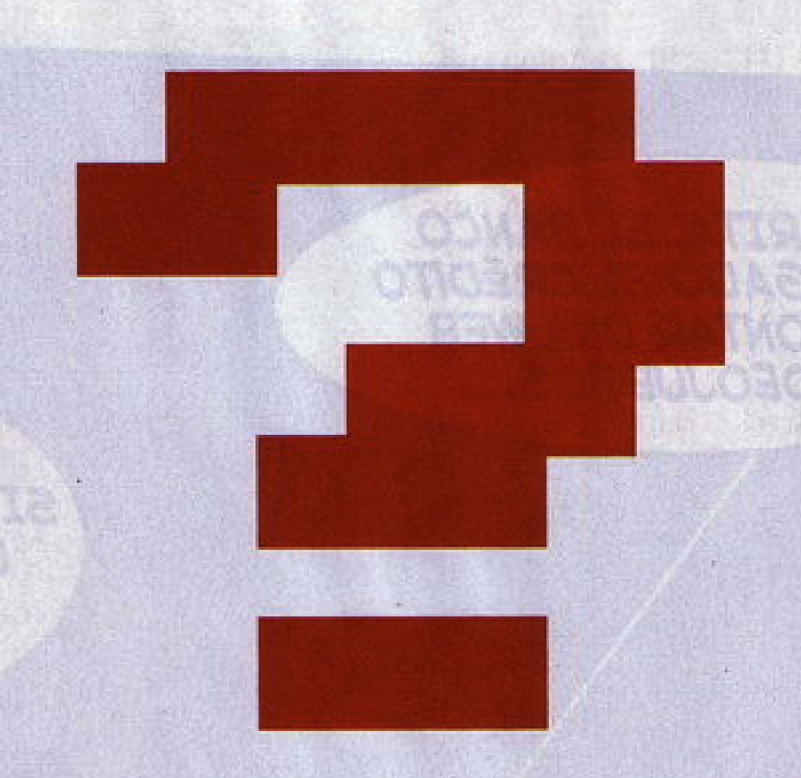
126

CRIATURITA, EL BANCO LE HA NEGADO EL CRÉDITO PARA MONTAR UNA WEB DE VIDEOJUEGOS...

LE HAN DICHO QUE SI HUBIERA SIDO PARA UN SEXSHOP ONLINE SE LO FIRMABAN EN 10 MINUTOS

Y QUE HABIENDO ANAITGAMES.COM QUE SE DEDIQUE A OTRA COSA

LLEGA ANAITTV, LA TELE DE ANAITGAMES



¿Ein?

¿Algo pasa en alg@RROBA?

¿Pero te lo creíste?

¿Ahora tendremos que cambiar algo de verdad?

A esperar tocan, otra vez.

Total, será lo de siempre, pero con otras letras y otros colorines. Pero ¿a que fastidia?

Freak Domain

Los Dioses deben estar locos II

¡Despelote de fotoblogs!

Que no es lo mismo que un desparrame, ¿eh? Bueno, de nuevo ración tremebunda de enlaces picantes para que la gente no se nos queje más de que antes esto molaba más porque había "culos y tetas", con perdón de la expresión. Todo sea por la nostalgia.

http://www.dailyniner.com/sabrinarose1.shtml
http://gorillamask.net/gm_media.php?show_page=gallery&page_id=15014
http://www.shermsshack.com/galleries/girl-next-door-ivy/index.php
http://z0d.com/ericaellyson1.shtml
http://novoporn.com/lachelle-marie/
http://www.asredas.com/url.php?id=29808
http://galleries.sexy-babes.tv/p/jana_mrhacova_feeling_tipsy/?nats=MTAyNzQ2OjI6Mg,0,0,0,1107877231
http://www.celebparasite.com/1272/Eva_longoria_is_smokin_hot_in_this_bebe_photoshoot.html
http://www.closepics.com/gallery/502/met_art/metart_busty_lucy/
http://dachix.com/babe-1162_Lisa+has+her+big+tits+covered+with+tissues.html
http://z0d.com/marta1.shtml
http://thousandbabes.com/perfect-shaped-blonde-tila-nguyen-posing-for-you
http://www.babeunion.com/gallery/amanda-hanshaw-boobs/
http://z0d.com/marta1.shtml
http://www.thesexblog.com/info/5178/kaylin-ryan
http://baberoad.com/galleries/nastydollars/bigtitsboss/tsi/0001/index.php
http://glam0ur.com/gals/angel_dark_and_lisen/index.php
http://64.46.38.232/hosted/photodromm_78/v45gh76uyi.htm
http://www.dailyniner.com/thumbs/iga1.jpg
http://hosted.met-art.com/Full_met-art_LUH_55_599/?pa=637705
http://ass.bodsforthemods.com/galleries/2008/2/penthouse_sunny_leone/index.php
http://www.dailyniner.com/nicoleaylward1.shtml
http://www.hasbabes.com/gallery/anette_dawn/anette_dawn_in_a_bikini
http://www.closepics.com/gallery/513/digital_dream_girl/super_hot_asian_katsumi/
http://hosted.goldinaraw.com/hel1_23012008/index.php?pa=1632136
http://galleries.pmates.com/galleries/digitaldesire/2008-02/Eufrat/
http://www.celebparasite.com/1240/Gemma_atkinson_is_hot_in_nuts_magazine.html
http://ass.bodsforthemods.com/galleries/2008/2/met_art_danae/index.php
http://www.celebparasite.com/1279/Keeley_hazell_is_hot_in_a_bikini_outside_in_london.html
http://novoporn.com/tiffy-fallon-green-lingerie/
http://www.babeupdate.com/galleries/2008/2/mc_nudes_stunning_beauty_micaela/
http://www.asredas.com/gallery/617/EroticaArchives/Erotic_Babe_Jenni_at_the_Beach/
http://www.hasbabes.com/gallery/katie_fey/sexy_teen_katie_fey
http://www.phun.org/index.php?navigation=hitman_girl
http://dachix.com/babe-1163_Ryder+Skye+smoking+hot+brunette.html
http://exgirlfriendmarket.com/delicious_young_babe_in_red
http://www.babeskickass.com/content/Trina_Michaels_in_green_lingerie/
http://www.kontraband.com/show/show.asp?ID=9900
http://glam0ur.com/gals/bree_olson/09/index.php
http://www.lettherebeporn.com/galleries/2008/1/playboy_playmate_xtra_sara_jean_underwood_2/index.php
http://www.closepics.com/gallery/509/danni/busty_brunette_ryder_skye_by_danni/
http://galleries.pmates.com/galleries/ftv/2007-12/valerie1_dream_hottie/
http://glam0ur.com/pics/10569.jpg
http://wwtdd.com/post.phtml?pk=3391
http://www.abc-celebs.com/gallerie_html/jenna_jameson_gallery2.htm
http://www.girlsofdesire.org/index.php?inc=1&gal_id=2992&count=1
http://z0d.com/ginajones3.shtml
http://glam0ur.com/gals/nikki_blond/100/index.php
http://www.babeunion.com/gallery/angel-dark/
http://www.shermsshack.com/galleries/sandra-nilsson/index.php
http://gorillamask.net/gm_media.php?show_page=gallery&page_id=14811
http://www.asredas.com/collection/Shay_Laren/
http://www.p0rnstars.com/porn/jenna-jameson.php

FRIKI GADGET

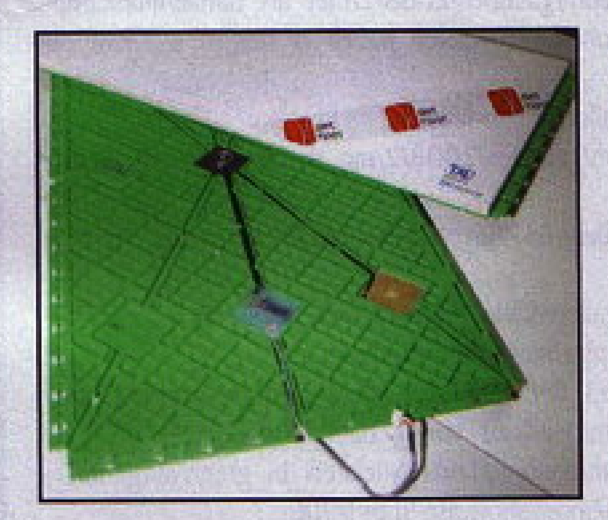
Hazte con estos productos antes de que tu vecino te los arrebate y luego se pavonee delante de tus narices. Que sabemos que te va mucho eso de competir, maníaco consumista. Todo sea por fomentar una comunidad de vecinos animada y entretenida.



El iPhone también se merece unos buenos altavoces

Y además de verdad, según sus poseedores, porque no es que el teléfono de Apple tenga buen altavoz integrado. Estos altavoces portátiles solucionan el problema, además con gran calidad de sonido y refuerzo de graves para que ya nadie se te queje de que tu flamante iPhone suena a lata.
http://dlo.com/products/portspeakers_iPHone_prod.tpl





El Gran Azulejo te vigila

Todavía es un prototipo, pero puede que dentro de un tiempo esté en todas las casas. Este azulejo de Tau Cerámica controla las veces que abrimos el frigorífico en busca de algo para picar, entre otras cosas. El objetivo parece ser que el azulejo nos regañe cuando nos pasemos con el chocolate y los refrescos, y cargarnos de culpabilidad por si no hay nadie en casa que nos haga ponernos a dieta. También puede servir para que en el comedor de la oficina la gente no se pase con el descanso para el cafelito. Agh.
http://www.coolest-gadgets.com/20080206/tau-ceramica-diet-floor/#more-11936



Solución sencilla pero útil

Si prefieres algo sencillo para cargar las pilas de tus mandos de Wii, hazte con este cargador que permite poner hasta 4 mandos de la consola de Nintendo. Ya no tienes ni que abrirlos para cargar las pilas, comodidad al poder.
http://www.joystiq.com/2008/02/07/react-recharge-dock-powers-4-wiimotes-for-50/



Escarabajo luchador RC

En cualquier lugar puede haber una épica batalla, cualquier criatura puede protagonizar una encarnizada lucha por la vida y el poder. Por ejemplo, un escarabajo. Sobre todo, si es por Radio Control. Movimientos realistas (camina con sus patas, ni ruedas ni nada parecido) y además incluye tronco de entrenamiento para que esté siempre listo para el combate.
http://www.locoria.com/escarabajo-luchador-rc-p-21.html?zenid=90f3f1c7d468363dac9260d8c39d6c0c







El floppy nunca pasa de moda

Antes que el Cd, estaba el floppy. Si guardas gratos recuerdos de los diskettes de baja que agujereabas para convertirlos en alta densidad para no gastar dinero, píllate estos Cds grabables con forma de floppy, y con 200 megas de capacidad. Mucho menos que un CD o un pendrive de hoy en día, pero la nostalgia es la nostalgia.
http://www.designboom.com/shop/floppydisk.html

Pantallón para el buga

Perdón por el anacronismo, no lo hemos podido evitar. Pero es que menudo aparato. Esta pantalla táctil de 7 pulgadas para nuestro CarPC lo tiene todo, sirve de dispositivo de entrada y puede reproducir películas en DVD y CD de música y muchas más posibilidades. Incluye amplificador de 55Wx4 con varias entradas de sonido.

http://www.xenarc.com/product/MDT-X7000.html







Marco digital con pantalla y media

Este nuevo marco digital de Mustek incorpora una segunda pantalla debajo de la principal, en la que podemos ver datos como la temperatura ambiental y la fecha y la hora. Ya que los marcos con widgets se nos escapan, soluciones rápidas y modestas como éstas pueden servirnos. Reproduce mp3, avi y mpeg desde cualquier tipo de tarjeta de datos.

http://gizmologia.com/2008/02/mustek-pf-e700-doble-pantalla-en-nuestro-marco-digital/#more-22203

Imprime sin cables

Se acabó eso de tener la impresora al ladito del ordenador, o tirando cables larguísimos por la casa o la oficina. La multifunción SCX-4500W de Samsung lleva, además de un montón de funciones y un diseño de lo más molón, Wi-Fi 802.11b/g y Ethernet 10/100. Que no quede dispositivo informático con cables, oiga.

http://www.engadget.com/2008/02/07/bonjour-scx-4500w-apples-favorite-samsung-multi-function-print/



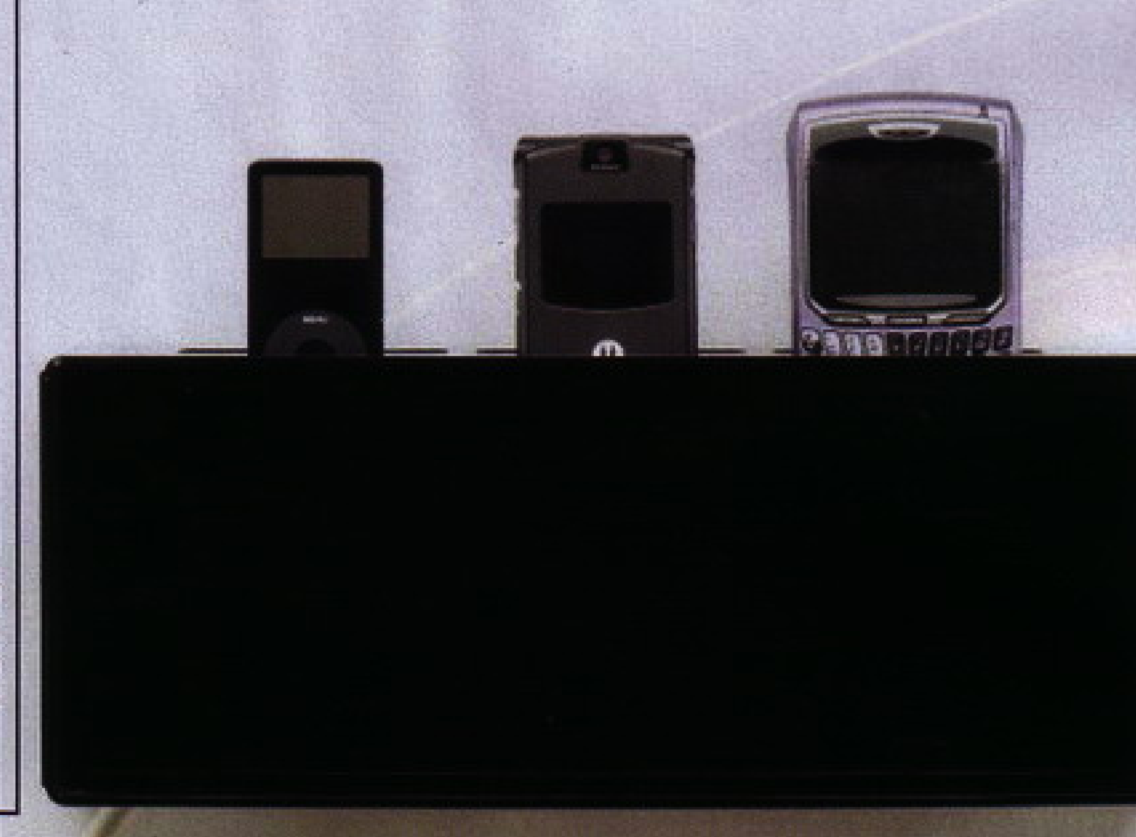




Una resolución estupenda para tus fotos de borrachera

Marcos digitales hay miles, eso está claro. Habrá que empezar a seleccionar y buscar la calidad sobre todas las cosas. Por ejemplo, este marco de Viewframe con pantalla de 8 pulgadas y resolución nada menos que de 800*480. Además de nuestras fotos más tiernas y embarazosas, reproduce vídeo mpeg 1, 2 y 4.

http://www.i4u.com/article14514.html



Carga tus cacharritos, tres exactamente

En vez de tener cargadores perdidos por la casa, este dispositivo que podemos atornillar a la pared, y de ahí a cualquier enchufe, puede salvarnos de más de un apuro. De diseño austero y poco llamativo, permite hasta tres cacharritos, y nada de cables colgando por la encimera o la mesa.

http://technabob.com/blog/2008/02/07/wall-charger-keeps-gadgets-organized/

Llega anaitTV

PLAYER 2 003243

El blog más elegante sobre videojuegos estrena plataforma de vídeo

La llamada web 2.0 tiene como primeros espadas a los blogs. O al menos es lo que entiende la gente, que ha abrazado la blogosfera o, mejor dicho, la ha creado con sus mejores esfuerzos. Lógicamente el frikismo ha invadido el mundo de los blogs y los fans videojuegos han entrado a saco creando docenas bitácoras con opiniones, reviews, noticias, trucos y todo tipo de desvaríos que han puesto en un aprieto a las revistas online especializadas en videojuegos. Que, curiosamente, en su día pusieron en un brete a las revistas impresas del sector. Relevo o no, los blogs sobre videojuegos tienen cada vez más peso y relevancia, y entre todos ellos destaca anaitgames.com, el blog de Xavi Robles, Pep Sánchez y compañía. Un blog que, ahora, estrena una original plataforma de vídeo que, seguro, no dejará indeferente a nadie con sus análisis y pensamientos sobre lo nuevo y lo no tan nuevo.



Elegantes al 100%

Anaitgames.com lleva ya un tiempo entre nosotros, y si ha destacado en el maremágnum de blogs sobre videojuegos ha sido por su particular forma de contar las noticias y rumores del sector. Un mundo más polarizado que nunca, en el que desafortunadamente muchos blogs con buenas intenciones han heredado el temible bagaje de los foros. O sea, los fanatismos y los malos modos, para empezar. Que no es que todos los foros sean cunas de malhablados y de fanáticos, pero suele pasar que lo malo se difunde mucho más y mejor que lo bueno y este caso es especialmente sangrante. Anaitgames ha demostrado que se puede hablar de videojuegos sin caer en extremismos y sin ser aburrido en el afán por evitarlo.

Recientemente, Anaitgames ha estrenado plataforma de vídeo online, anaitTV. Desde luego, no es Gametrailers.com, cosa que reconocen. Pero es que tampoco hace falta. Es decir, no necesitamos otro Gametrailers.com, no hay que hacer lo de siempre. El caso es hacer lo que a uno le apetezca a la hora de hablar de juegos. Y en el caso de Anaitgames hay mucho de que hablar. Y bueno. Esperemos que, con el tiempo, el boca a boca y el consiguiente aumento de prestigio, Anaitgames no caiga en el fenómeno que hemos visto en otras páginas web. A medida que aumenta el contacto con los departamentos de prensa y demás, hay quien ha optado por suavizar su mensaje en pro de la comercialidad. Hay quien directamente ha cambiado su mensaje, pero no es el momento para discutirlo. Ojalá Anaitgames siga conservando su frescura (a pesar de que la frase en sí ya está de lo más manida) y su independencia. Prueba de ello es la primera entrega de AnaitTV. No podemos sino recomendar la visita diaria a el blog más elegante sobre videojuegos. Que cunda el ejemplo de Anaitgames.<





WEB del mes

http://www.capnwacky.com/lists/list67.html

Seguro que eres todo un hacha en las compras y subastas online, y que no solo te pateas este mundillo como Pedro por su casa, sino que además te has creado toda una reputación de buen y honesto vendedor/comprador, ¿verdad? Pero no siempre es así. Siempre hay desalmados que timan al personal cuando pueden, o bien hay gente que compra por comprar y luego vienen los malos ratos y los desaires en forma de mensajes y votos negativos. De todo hay en la viña de eBay, puede decirse. Y todo tipo de mensajes se pueden encontrar en esta austera pero entretenida página, que recoge feedback en positivo y negativo de toda clase de subastas... Y de toda clase de personas. Entre los mensajes positivos podemos leer "el producto llegó pronto, desde entonces tengo sueños eróticos con el vendedor. Gracias" o "el embalaje color marrón corriente engañó a mi esposa", y entre los negativos "este perro no caza", "esta fiambrera de Espacio 1999 que compré no ha llenado el vacío de mi vida como yo esperaba" o "a pesar haber seguido las indicaciones, no he podido introducir el objeto en ninguna de mis cavidades corporales". Dios bendiga Internet y eBay. *

Unusual eBay Feedback

By BRODIE H. BROCKIE, JUSTIN VIDOVIC, BEN FLASTER, and GUTBLOOM

POSITIVE: Item shipped quickly, have been having erotic dreams about seller. Thanks!

POSITIVE: Thanks for great Rainbow Brite lunchbox. Should shrunken head be inside?

NEUTRAL: Excellent communication, but should've poked holes in box before shipping the kitten. Refunded.

NEGATIVE: Despite indication in listing, I could not fit item into any of my body cavities.

NEGATIVE: Honda R-Type sticker did not add horsepower as advertised.

NEUTRAL: Item shipped promptly and in good condition, but I should not have to bid on birthday presents from my parents.

POSITIVE: I don't really remember what I ordered. But I've been sitting in the box it came in all day, and it's great!

NEGATIVE: Product didn't work, possibly broken. I woke up this morning and was disappointed to find I still believe in Jesus Christ our Savior. :(

POSITIVE: Excellent Buyer. A++++++. Thrilled by the quartz movement of the "Rolex". HIGHLY RECOMMENDED.

NEGATIVE: Should have been clearer that seller only accepts payment in Bhats via Eastern Union Moneygram.

POSITIVE: Plain brown packaging seemed to fool my wife. Thanks!

NEGATIVE: The dog won't hunt.

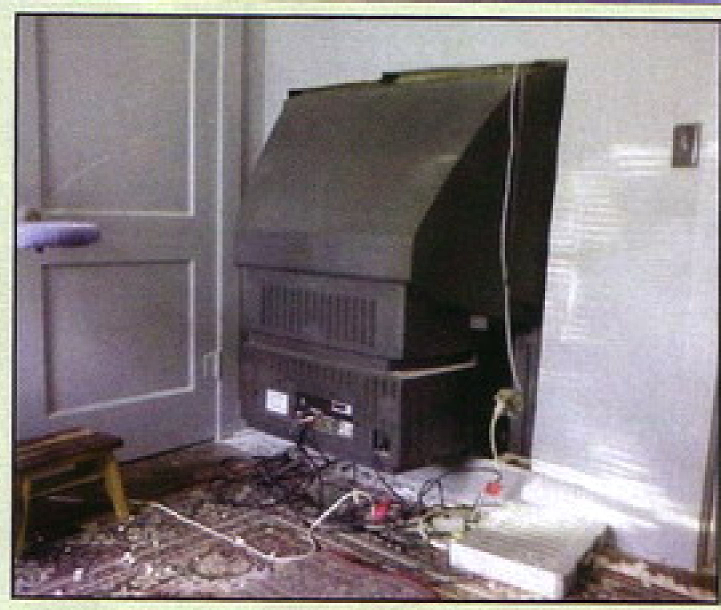
NEGATIVE: Very nice monkey mascot costume, but it's a size 34, not a 63 as advertised.

WEB Chorra

http://chorradas.rebuscando.info/2008/01/24/ghetto-flatscreen/



A ver. Una cosa es resolver con ingenio los problemas de espacio de las viviendas actuales, sobre todo en relación a nuestras necesidades de ocio y tecnología. Pero otra es ser, directamente, una mala bestia. O todo un genio, según se mire. Véase el ejemplo de la web chorra de este mes. Alguien que no quiere (o no puede) gastarse un dinero en una tele LCD o de plasma, y que además tiene problemas de estrecheces en el salón con la tele CRT que tiene actualmente. Ambos problemas se pueden resolver... Agujereando la pared, pero del todo. Vamos, abriendo un boquete por el que pueda caber el inmenso e imponente trasero de nuestra vetusta tele. Si alguien no lo cree, que eche un ojo a estas fotos, porque no solo es posible, sino que alguien lo ha llevado a la realidad. Seguramente el cuarto damnificado (o sea, el que recibe el culo de la tele) sea el de la plancha o el de algún miembro familiar no muy bien considerado. Eso sí, no se puede decir que la tele no ventile, si es que tiene un cuarto entero para respirar... *





"Hum, así que en eBay no solo pueden encontrarse juegos antiguos a precios desorbitados. y abusivos...": Gaby López

arroba1@megamultimedia.com, ya estáis tardando

TODO para tu MOVIL

SONIDOS REALES

Envía **RRREAL** seguido del código de tu sonido real al **7775**
Ej.: RRREAL 6401 o llama al **806 506 918**

ABUELA	8089	BISBAL	8230	CONDUCTOR	8204
ACETATE	8244	BOLLERA	8237	CORRECAMINOS	8224
ALBAÑIL	8221	BORIS	8129	CORRER	8222
AMANTE	8090	BORRACHO	8146	CRUZ Y RAYA (SONAR)	8147
ANUNCIO ONCE GUIRIS	8241	BURLA	8235	CUCO	8276
APLAUSOS	8282	CABALLO	8279	DABADABADO	8219
ARTURO FERNÁNDEZ	8100	CAMELLO	8231	DAVID DE MARIA	8189
AUSTRONAUTA	8205	CAMILO SEXTO	8131	DESTROZADO	8217
AVIONETA	8281	CAMPEONES	8095	DINIO	8105
AZNAR	8112	CANARIO	8277	DISPAROS	8275
BART SIMPSON	8240	CARMEN DE MAIRENA	8126	DOCTOR MALIGNO	8199
BEBE	8239	CATETA	8097	DON OMAR	8218
BEBE GRITO	8116	CHIQUITO	8104	EL PADRINO	8195
BESO	8280	CISTERNA	8278	EL REY	8207
BESO CARTOON	8238	COMIC	8228	EN LA SELVA	8274

SONIDOS POLIFONICOS

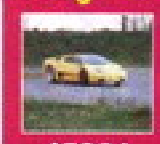
Nº Licencia SGAE: SGAERMV&M 35/581/06/80406

Envía **RRPOLI** seguido del código de tu polifónico al **7775**
Ej.: RRPOLI 6401 o llama al **806 506 918**

AVENTURA - LA GUERRA	70442	PAULINA RUBIO - DAME OTRO TEQUILA	70470
CHAMBAO - POKITO A POKO	70444	DAVID MARIA - LA CIUDAD PERDIDA	70455
HOOBASTANK - DISAPPEAR	70445	HOMBRES G - NO LO SE	70457
IGUANA TANGO - VOLVERAS	70446	JIMMY BAD BOY - BAILANDO	70458
JARABE DE PALO - 1M2	70447	LOS PECES - MERODEANDO	70460
PSYCHEDELIC SALLY - COCACOLA	70449	LUCA DI RISIO - CALMA Y SANGRE FRIA	70461
RAFAELLA C.- HAY QUE VENIR AL SUR	70450	MARIAH C.- WE BELONG TOGETHER	70462
ROSANA - AQUEL CORAZON	70451	MARC ANTHONY - VALIO LA PENA	7930
ZINO Y LENNOX - BANDIDA	70452	MAREA - LA RUECA	7931
BRISA - LA MUSICALITE	70464	MELENDI - MI RUMBITA PA TUS PIES	7932
CRAZY FROG - AXEL F (CRAZY FROG)	70465	AVENTURA - AMOR DE MADRE	7933
EL CANTO DEL LOCO - CONTIGO	70466	BRITNEY SPEARS - MY PREROGATIVE	7934
FRANZ FERDINAND - THIS FIRE	70467	MELENDI - UN RECUERDO QUE OLVIDAR	7941
JULIETA VENEGAS - OLEADA	70468	EMINEM - BUSINESS	7936
LA QUINTA ESTACIÓN - PERDICIÓN	70469	BOB MARLEY - GET UP STAND UP	7848

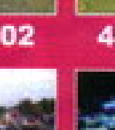
VIDEOS

Envía **RRVIDEO** seguido del código del vídeo elegido al **7775**



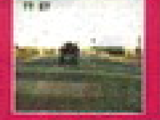


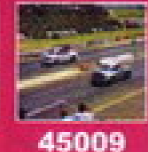
45001 45002 45003



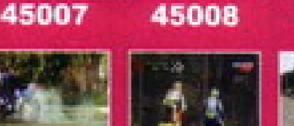


45004 45005 45006





45007 45008 45009



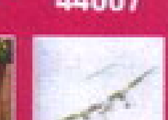


44001 44002 44003





44004 44006 44007

42011 42009 42005

Coste del SMS: 1,20 euros IVA no incluido. (Requisitos para la descarga de contenidos: 2 sms para fotos color y videos). Coste llamada 806: Red Fija 1,16 euros/minuto; Red Móvil 1,51 euros/minuto, IVA incluido. Coste conexión wap según operador y a cargo del usuario. Sus datos serán incluidos en un Fichero titularidad de Jetcomcell S.L. para la gestión del servicio de Contenidos SMS, y para ofrecerle promociones futuras.

Para acceso, cancelación, rectificación y oposición: Apartado de Correos 14953 - Madrid 28080.

Todos los contenidos son para móviles wap compatibles con fondos a color y videos.

DINAMICOS

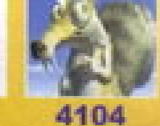
Envía **RRDINA** seguido del código del DINAMICO elegido al **7775**



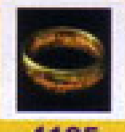
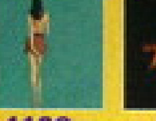


4394 4395 4398





4603 4614 4104

4105 4108 4109

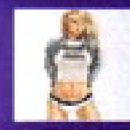
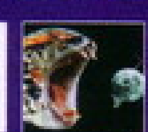
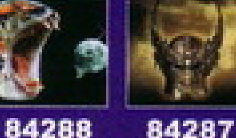


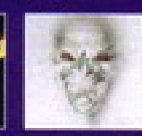


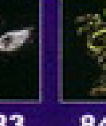
4111 4160 4161

FONDOS

Envía **RRFOTO** seguido del código de tu polifónico al **7775** - Ej.: RRFOTO 64601 o llama al **806 506 918**

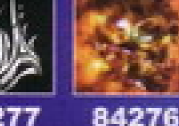


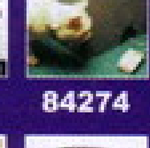
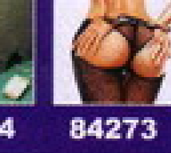




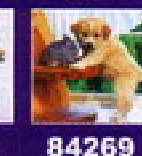
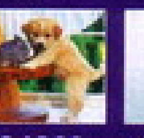


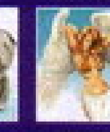
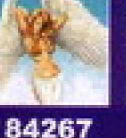




84289 84288 84287 84286 84285 84284 84283 84282 84281 84280 84279 84278 84277 84276



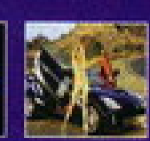



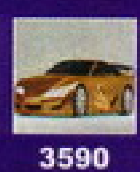


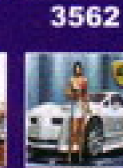





84275 84274 84273 84272 84271 84270 84269 84268 84267 84266 82563 3343 3373 3493

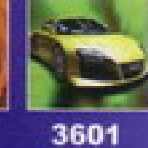





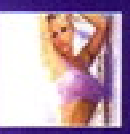




3536 3539 3543 3545 3546 3548 3550 3562 3563 3568 3572 3576 3579 3584

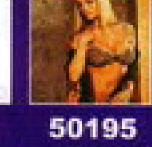
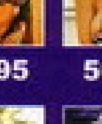
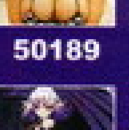
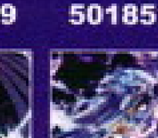
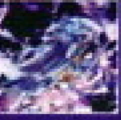
3585 3586 3587 3588 3590 3591 3592 3595 3596 3597 3598 3599 3600 3601

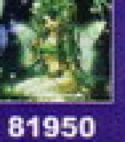









5326 50227 50223 50220 50219 50228 562 50218 50195 50189 50185 5959 81734 81736

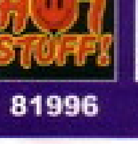
81737 81738 81742 81743 81744 81745 81944 81945 81946 81947 81948 81949 81950 81952



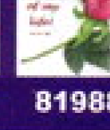














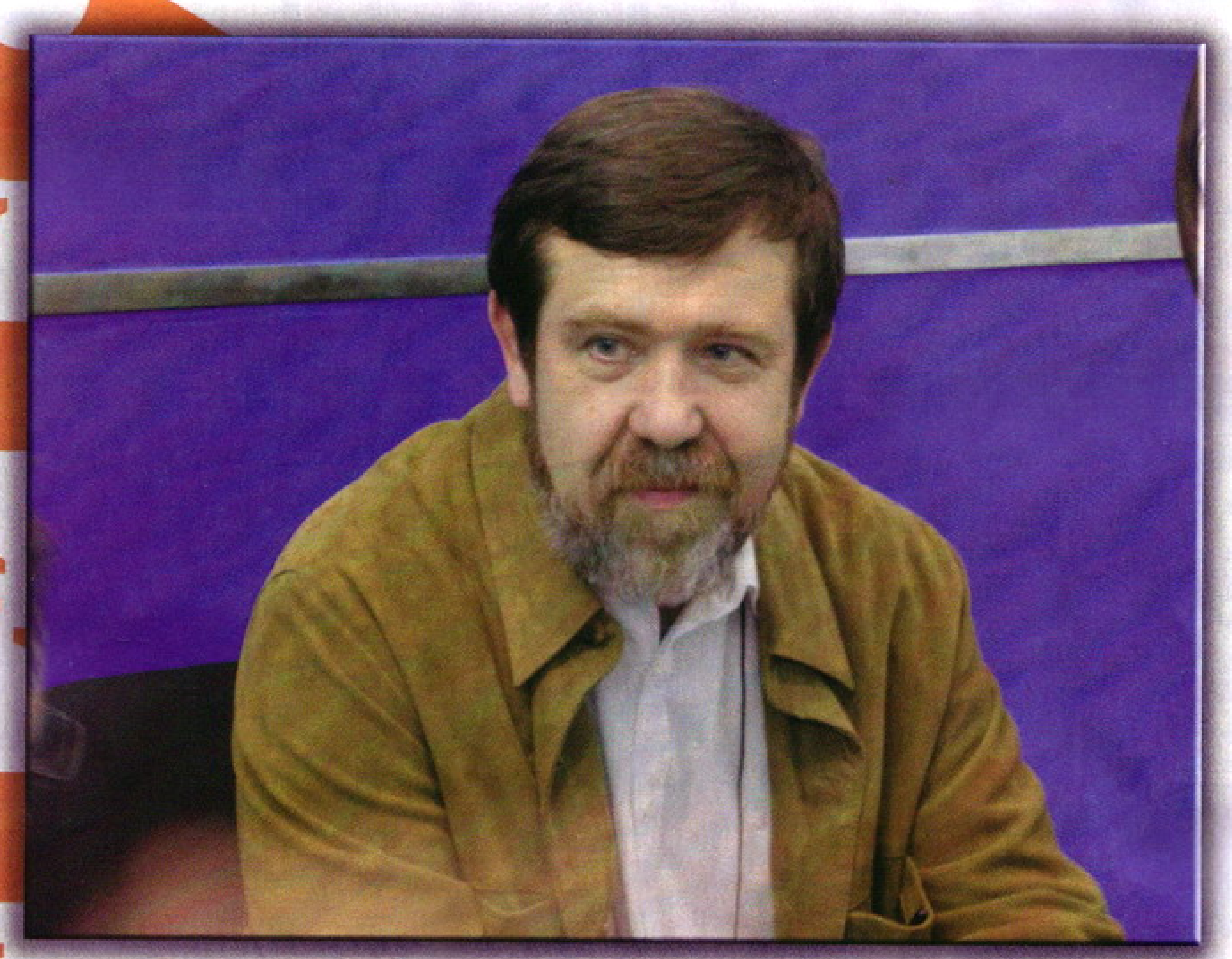



82047 82046 82026 82019 81999 81996 81993 81992 81988 81985 8256 8341 8459 8470

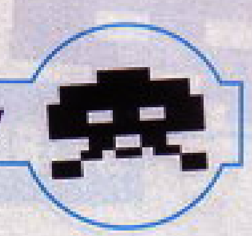
El pasado 15 de enero Alexey Pajitnov tuvo a bien de ofrecer una conferencia en la Universidad Autónoma de Barcelona en el campus de Cerdanyola del Vallés, incluida dentro de unas mastodónticas jornadas sobre videojuegos, unas actividades académicas enmarcadas dentro de la semana dedicada de la Universidad referente al Año de la Computación que celebran. Y ahí estuvimos, sí señor.

ALEXEY PAJITNOV, EL PAPÁ DEL TETRIS

Un encuentro en Barcelona



"Cuando los niños escuchan a Tchaikowsky dicen '¡Tetris! ¡Tetris!"



And the Oscar© goes to...

Con ánimo escacharrado como cuando uno ha contado mil veces la misma batallita, con tono cómodo y arrastrado, alargando cualquier explicación, con profesionalidad adquirida de saber qué contar, qué callarse o qué dejar en el aire con la seguridad de que su sincera y campechana presencia es suficiente crédito para que el entrevistador sea amable cuando se siente delante del ordenador para transcribir sus palabras. Nadie se atrevería a vilipendiar a Alexey Pajitnov, el ruso es buena gente, simpaticote, se hace querer. Para su desdicha yo no me hago querer, no soy simpaticote y no sé si soy buena gente. Y no soy ruso.

No es que Alexey -permítanme que le tutée- merezca ser enviado a Siberia a picar hielo por no contarnos toda la verdad y sólo la verdad, no, el hombre nos cuenta lo que queremos oir y no nos miente, no nos engaña. No queriendo, al menos. Le pudimos hacer preguntas tanto en público como en privado y en su ortodoxa paciencia nos respondió sonriente, divertido y en momentos agradecido por no exponerle por enésima vez las preguntas que los medios siempre le hacen, ya saben, que cual es su récord de lineas, que cómo se inspiro para hacer el Tetriš o qué hay de cierto en la agria polémica que tuvo con Iñaki Gabilondo, que le preguntaría Ramón Arangüena.

Lo destacable del caso es el máximo exponente de la mentalidad productiva soviética que Alexey muestra y su encarnación como ruso del siglo XXI. Su porte, su presencia, su verbo y su obra enfatizan el factor perdurabilidad de lo soviético, en lo intelectual y en lo material. Vestido con una chaquetilla color camello, camisa rasa, pantalones oscuros y calzado a camino entre zapatilla de ir por casa y mocasín sport, muy familiar, demasiado natural para resultar artificialmente socialista, poco habitual para una persona con la vida solucionada y con dinerito, un proto-hombre de familia medio-alta que no se deshace de sus orígenes comunistas, aunque fueran impuestos. Su obra magna, el Tetris, también es así, perdura y durará, un juego humilde que se cuela en toda super máquina de entretenimiento, por muy hi-tech que sea. Nos habló de su creación pero también le preguntamos sobre su persona.

Bienvenidos, hijos del rock'n roll

"Hola, saludos a todo el mundo y gracias por venir. Mi nombre es Alexey Pajitnov y, francamente, no entiendo porque estoy aquí exactamente, no tengo nada realmente importante que decir ni un mensaje serio que transmitir." Así empezó su exposición y durante media horita nos contó la batallita de los orígenes del Tetris, omitiendo asuntos escabrosillos como el destino de sus compañeros de equipo con los que desarrolló el Tetris que se propagó por toda Europa primero y por todo el planeta después, o el culebrón de permisos, copiadas y litigios con Mirrorsoft, Atari, Nintendo y otras. Su intención era entretenernos, no asustarnos.

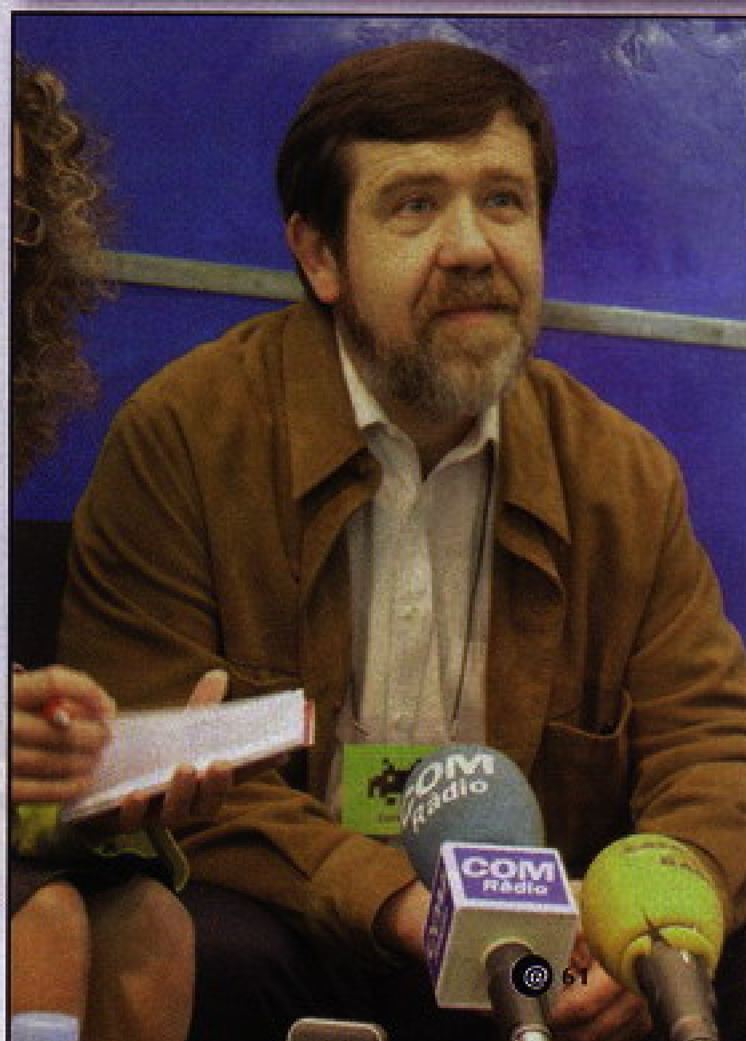
No se entretuvo en detalles técnicos ni tampoco quisimos incomodarle con ellos, suficiente cara de susto puso cuando quien ahora les escribe le planto un disquette de 8 pulgadas delante de sus narices para que lo autografiara y el ruso comentó que ese formato era el que utilizaba en el ordenador Electronika-60 con el que ingenió un primigenio Tetris. KGB still watching you, Alexey.

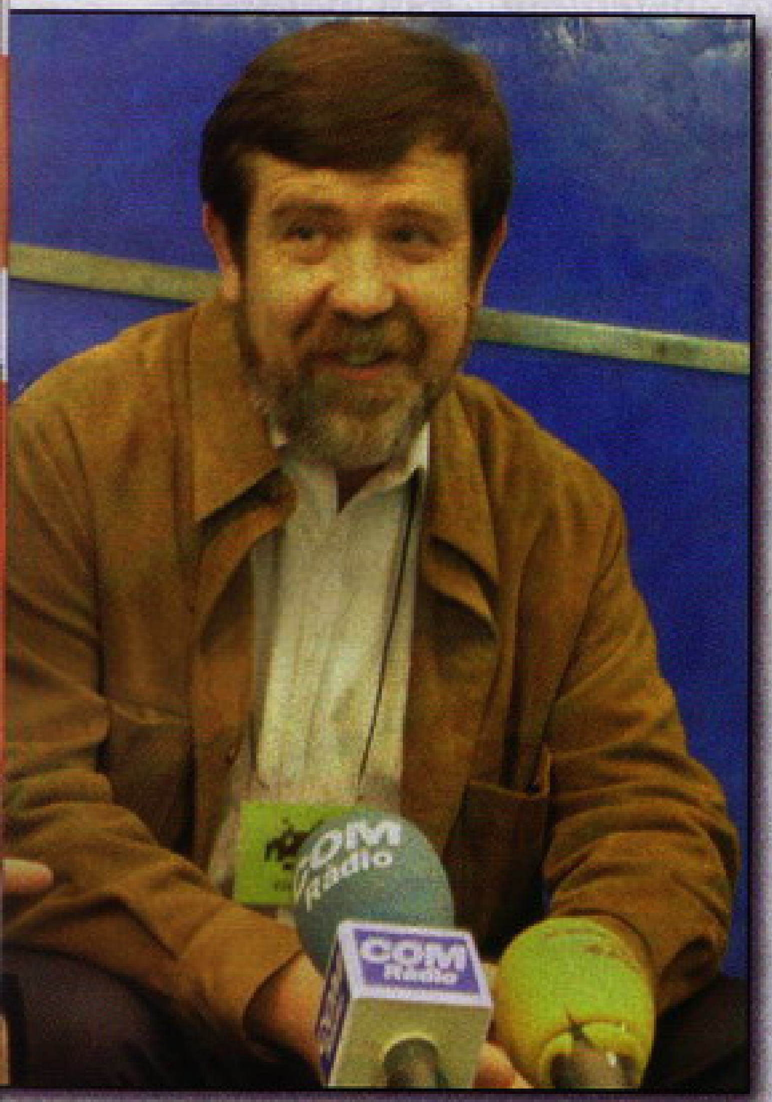
Era inevitable que apareciera el tema Pentaminó, el puzzle con el que había jugado en su infancia y en el que se basó para crear el Tetris. *"Se me ocurrió pasarlo al ordenador sin ningún tipo de preparación, sin ningún organigrama y sin comentarlo a nadie de mi equipo. Lo implementé para ver si funcionaba sin tener en cuenta ninguna opción de rotación de las piezas. Puede sonar ridículo ahora pero hemos de tener en cuenta que era el año 1984 cuando empecé con el Tetris y los ordenadores que teníamos no tenían ningún tipo de modo gráfico, la pantalla era de 30 lineas y 80 columnas y sólo símbolos alfanuméricos, tuve que utilizar símbolos, corchetes para simular piezas cuadradas, así creé las figuras."* Lo que no queda muy claro es si el Pentaminó persistía en su memoria o si, por contra, fué un recordatorio posterior o acaso una inspiración oportuna: *"Vi la descripción detallada del juego Pentaminó, entre otros, en un libro del Profesor Solomon Golomb de la Universidad de Michigan"* declaraba pocos minutos después.

Logros como la penicilina o los PostIt resultaron casuales o casi, implementaciones un poco como a la sopa boba; el Tetris no iba a ser un excepción: *"Mi intención era simular un juego de tablero en el que dos jugadores pusieran sus fichas por turnos, que cada uno pudiera rotarlas, girarlas y ponerlas en la posición que quisieran. Mantener las piezas del Pentaminó daba como resultado un juego demasiado largo y aburrido y lo que yo buscaba era algo dinámico, en tiempo real, así que simplifiqué las fichas a tetraminós. La siguiente simplificación que hice fué la de eliminar*

"MI NOMBRE ES ALEXEY PAJITNOV Y NO ENTIENDO PORQUÉ ESTOY AQUÍ EXACTAMENTE"







"MI INTENCIÓN ERA SIMULAR UN JUEGO DE TABLERO EN EL QUE DOS JUGADORES PUSIERAN SUS FICHAS POR TURNOS"

la opción de girar, la del reflejo de las fichas; lo que hice fué añadir fichas que resultasen el reflejo de las que se podían girar, así también resultaba más fácil de jugar, ya que se eliminaba la opción de reflejo. Luego decidí - ya que no tenía la opción de dos jugadores- que podía poner las fichas que cayeran por efecto de la gravedad de arriba a abajo de una forma natural. No recuerdo en qué momento exacto pensé en esa implementación de que las piezas cayeran." ¿Demasiado vodka en el desayuno, quizá?

"En el momento que realicé mi versión de 30 lineas me di cuenta de que rellenaba muy rápido, en 15 segundos se acababa la partida, demasiado corto para un juego. Se me ocurrió poner un scroll vertical pero no tenía suficiente memoria en el ordenador. En ese momento ese Tetris ocupaba 27Kb de memoria; hoy en día cualquiera de vosotros ya los utiliza enviando un e-mail. Por la falta de espacio en pantalla se me ocurrió hacer desaparecer las lineas que ya estaban completadas y así poder seguir jugando. Y esta es la historia del Tetris" y así terminaba un trabajo de tres semanas. El resto de atributos del programa como puntuaciones, niveles y demás se hizo mucho después y Alexey reconoce no recordar muy bien cómo lo hizo pero sí que le suena que fué una parte muy fácil de hacer. La parte más dura fué terminarlo porque una vez el programa principal estaba hecho se pasaba más tiempo jugando que no pensando como terminarlo, se excusaba a mí mismo diciendo que lo estaba probando pero finalmente se puso manos a la obra, acabó el código, *"puse alguna decoración en pantalla y enseñé el juego a mis amigos, quienes se volvieron locos al verlo y se engancharon sin remedio, y me di cuenta de que no era yo, que todo el mundo se volvía loco con el juego"* explica así tal cual, como un Abuelo Cebolleta al uso.



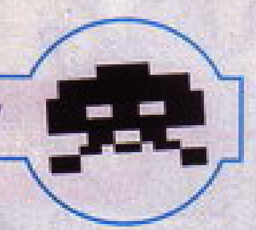
Tres tristes Tetris

Entre conferencia, charlas y entrevistas, Alexey nos llegó a insinuar tres teorias distintas que explicarían el éxito del Tetris, cada cual igual de creible, por supuesto.

"No creo que exista una única teoría para explicar el éxito del Tetris" empezó diciéndonos. *"mucha gente argumenta que llegó en el momento justo en la historia de la informática porque la gente, hasta ese entonces, tenía una barrera para empezar a trabajar cómodamente con ordenadores personales. Eran máquinas complidas y sólo los especialistas eran capaces de entenderlas y saberlas utilizar, así que cuando la gente vió que el juego eran tan fácil y natural de jugar, de alguna manera se rompió el hielo y eso supuso un punto de inflexión muy importante. Me gusta esa teoría pero si es correcta o no, no lo sé."*

Siguiendo con su imitación dialéctica de Groucho Marx de cuando decía aquello de que si no les gusta su opinión, tranquilos, que tenía otra, elucubró: *"Otra sugerente teoría sobre el éxito del Tetris dice que lo que ves en pantalla son ni más ni menos que el rastro de tus propios errores, ya que los logros, el completar lineas, se borran de la pantalla y todo lo que queda son los horribles agujeros, por eso sientes el ansia de arreglarlo y seguir jugando."*

Sacándole más punta a las teorías del éxito, esta vez con inocente discriminación de género humano, respondió que *"no creo que el Tetris sea específico para las mujeres. Creo que Tetris gusta a la mujeres porque en el juego se crea, se construye algo, por contra los shoot'm-up consisten en destruir. Probablemente la simplicidad es el secreto por lo que gusta a las mujeres."* Y por lo que gusta a todo el mundo, podríamos decir, ya que frase subordinada *'El secreto del Tetris está en la simplici-*



dad' es en la que más veces insistió. En comparación a otros juegos como Pong, Space Invaders, Galaxian o Pac-Man, declaró que *"no creo que Tetris sea mejor que otros juegos, especialmente yo estaba enganchado al Pac-Man y siempre ha sido uno de mis juegos favoritos. La diferencia entre Tetris y el resto de juegos probablemente sea que juegos como Pac-Man siguen teniendo un espíritu ubicado en un propio tiempo con sus gráficos característicos y todo eso, mientras que Tetris es más abstracto, más atemporal."*

Los viejos buenos tiempos

Alexey se muestra ciertamente neutral y tal vez un poco positivista cuando opina sobre máquinas y videojuegos actuales. *"Juego mucho, pruebo todos los juegos tipo puzzle o de rompecabezas que encuentro. He jugado mucho al Civilization o al World of Warcraft y me lo he pasado muy bien"* nos comentaba, o *"cualquier plataforma es buena para hacer juegos. El hecho de poner tener varios tipos de máquinas es lo que resulta interesante"*; incluso se atreve con vaticinios con ojo de buen cubero: *"Los nuevos juegos que se harán se acomodarán más y mejor a las máquinas sobre las que se crearán pero también creo que los juegos serán esencialmente los mismos que les gusta a la gente porque aunque el hardware cambia muy rápidamente, el cerebro humano no, sigue siendo el mismo y eso ha sido así en los últimos 20 años, así que se seguirán haciendo buenos juegos."*

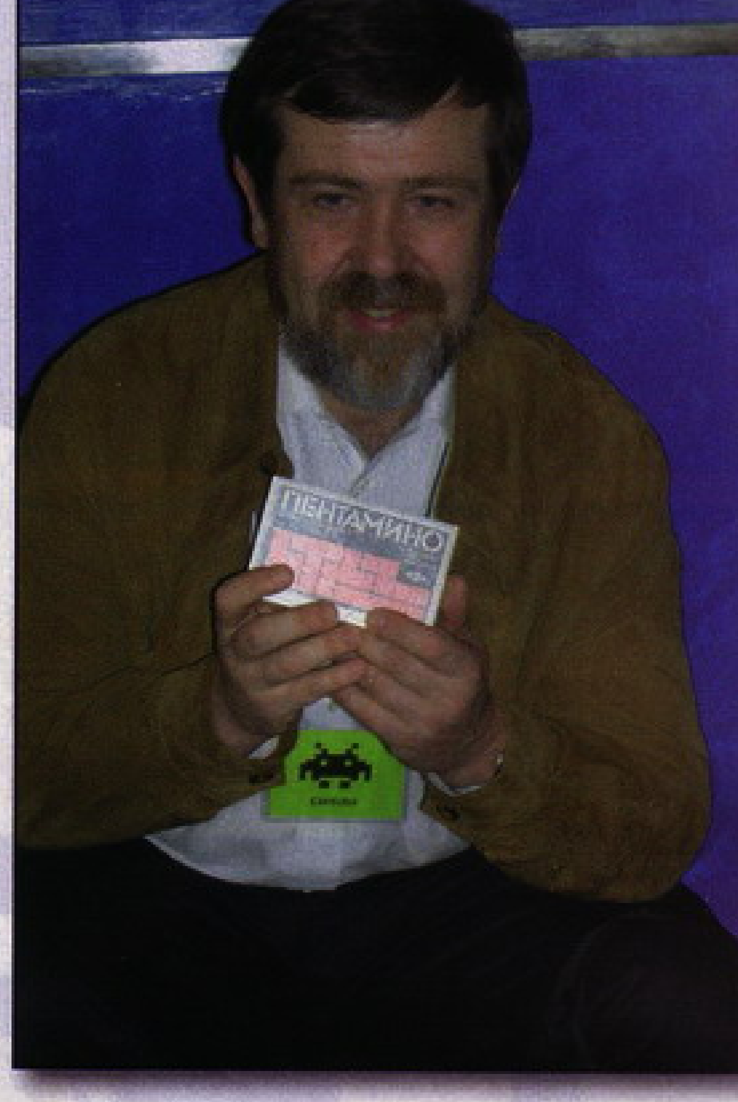
Pero la cabra tira al monte, defiende lo suyo con numantino acierto. *"Ante todo me gusta mi propia versión, por supuesto [risas]. Me gusta mucho la versión de GameBoy, es la que se acerca más al concepto original. También me gusta mucho la versión on-line, que es la que más juego. Y sí, juego al Tetris habitualmente. La verdad es que forma parte de mi trabajo, he de aprobar la mayoría de versiones que se hacen del juego para distintas plataformas, soy adicto al juego, me encanta, al menos juego media hora cada día jugando al Tetris. Y no veo nada de malo en ello. Durante 25 años he estado oyendo que no es sano. Nunca me han confirmado que el juego resulte dañino para nadie. Los juegos de violencia u otros rompecabezas tampoco."* Alexey ha de defender su postura, se gana las habichuelas trabajando actualmente para Microsoft, aunque, bueno, *"ahora no trabajo mucho, francamente. Tengo distintos grupos a los que les gusta implementar algunas de mis ideas. A veces hacemos juegos pequeños"* nos contaba refiriéndonos a amiguitos que tiene en San Petersburgo. Y es que es normal que haga lo que le sale del arco del triunfo, su empresa Tetris Company le reporta unos beneficios brutales, sólo con royalties de la marca no me caben los números en la cabeza.

Hace hincapié en el estilo de vida capitalista cuando nos recordaba que *"en esos años la industria del software no existía en la Unión Soviética, no se podía comercializar ningún programa. La única forma para que los programas científicos, las herramientas informáticas o los juegos circulasen era distribuyéndo copias de pago a tus amigos, esa era la única manera. Era un poco preocupante porque sólo podías vender dos o tres veces un programa, en muy poco tiempo se lo copiaba todo el mundo. Esa era la realidad, probablemente eso contribuyó a la expansión del juego y que se hiciera popular"* y con semblante serio nos recrimina cuando nos confiesa que cree que *"la gente no gasta lo suficiente en videojuegos, podrían gastar mucho más. La gente se gasta tranquilamente 6 ó 7 euros en una entrada de cine para ver películas estúpidas que duran dos horas pero no gastan más de una media de 20 céntimos por juegos on-line o de descarga o incluso de compra física. No es justo."*



Rompecocos y cascanueces

Los puzzles, rompecabezas y acertijos siempre han apasionado al bueno de Alexey, siempre que tenía ocasión o una excusa para programar alguno lo hacía. Actualmente cree que *"la mayoría de juegos de tablero ya tienen su versión en videojuego. No obstante creo que el juego japonés de mesa GO no está muy bien implementado todavía"* y no echa de menos juegos físicos como el Pentaminó, Tangram o el Cubo de Rubik -el clásico, no el nuevo Rubik's Revolution- porque Alexey sigue dale que te pego, *"hace poco he completado un cubo de Rubik, el de 5x5x5 piezas, que es complicadísimo, un gran desafío"* nos decía con una sonrisa de oreja a oreja.



"AHORA NO TRABAJO MUCHO, FRANCAMENTE"

Alexey Pajitnov es consciente de que ha creado un mito o que al menos él es la base de que lo sea. *"Cuando los niños escuchan a Tchaikowsky dicen '¡Tetris! ¡Tetris!'. No fué idea mía la de poner ese tipo de músicas rusas, pero me gusta la elección, sí, me gusta. La estética soviética del conjunto no me convence del todo pero si los expertos en marketing consideraron que era apropiado para una correcta comercialización, lo acepto, que Tetris no es solamente para que yo me lo pase bien, es para el mercado. Aún y así no hay nada malo en ello, no son más que estereotipos como lo son en la mayoría de campañas de publicidad"*. Todavía no ha visto un juego que pueda ser el sucesor del Tetris como juego que deje huella por su efectividad y simplicidad pero tiene la esperanza de que aparezca algún día. Si alguno de ustedes ha creido ver un videojuego que pueda ser el próximo protagonista en el gran libro de la Historia y de la Cultura del videojuego, se lo ruego, pásense por www.matranet.net y pónganse en contacto con S.T.A.R., que soy yo por si no se habían dado cuenta, que le pasaré el dato al simpático de Alexey, a ver qué cara pone.

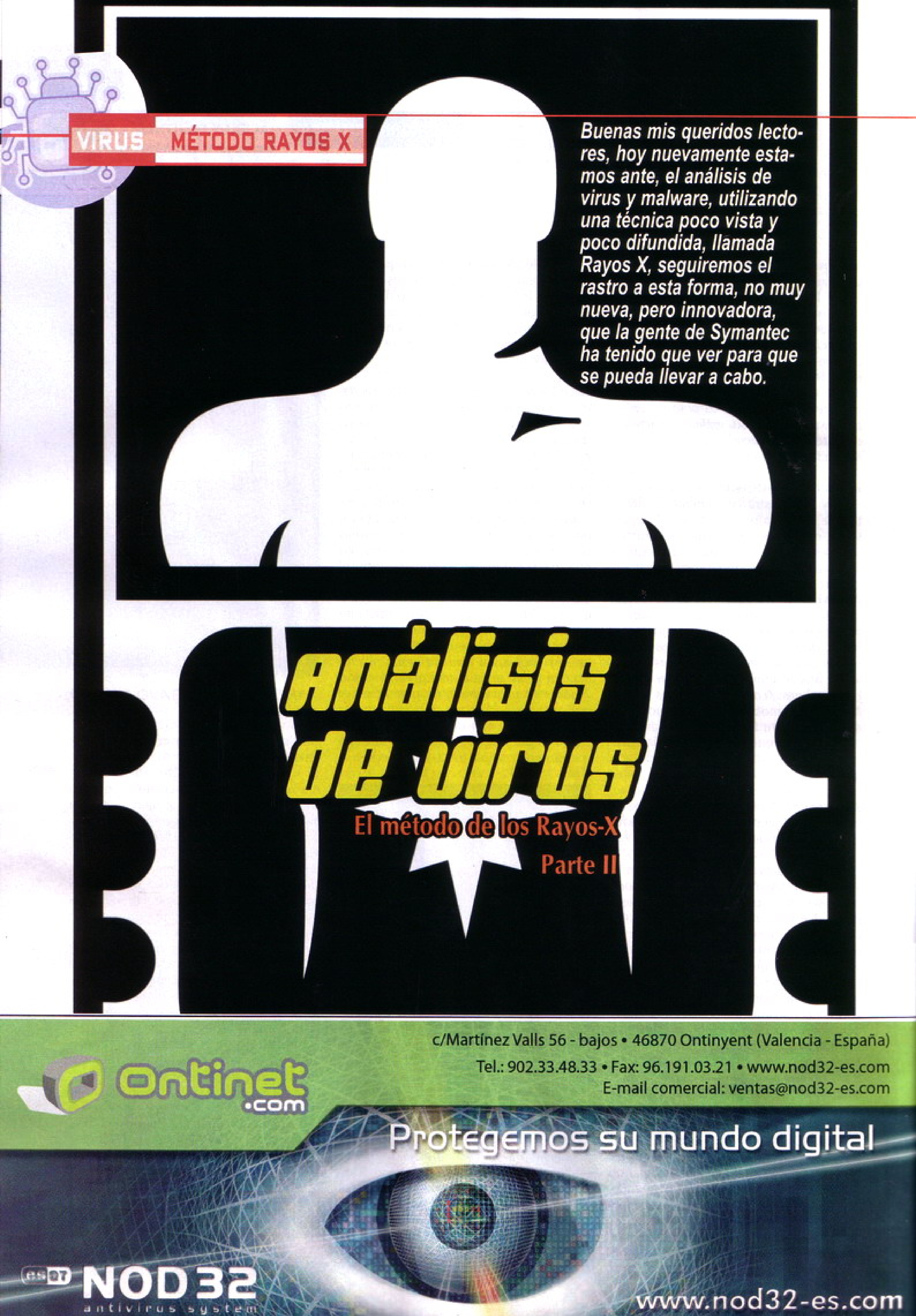
S.T.A.R.<

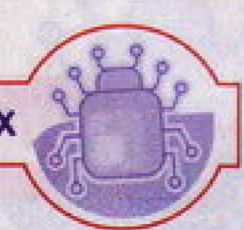
Análisis de virus

El método de los Rayos-X

Parte II

Buenas mis queridos lectores, hoy nuevamente estamos ante, el análisis de virus y malware, utilizando una técnica poco vista y poco difundida, llamada Rayos X, seguiremos el rastro a esta forma, no muy nueva, pero innovadora, que la gente de Symantec ha tenido que ver para que se pueda llevar a cabo.





¿En qué nos quedamos?

Bien, habíamos quedado en el análisis de una parte del virus

```
start:
        mov bx,virus-
length
        mov bp,offset
start
decrypt_loop:
        add byte ptr
[ bp+0Ch],33h
         inc bp
         dec bx
         jnz
decrypt_loop
```

El registro BX contiene la longitud del código a cifrar, y BP contiene el puntero para saber desde donde se empezará.

En la tercer línea tendremos BP + 0Ch, que se trata de la posición de memoria donde encriptaremos en cada iteración. Es decir, lo que vale BP más una constante definida.

Luego el incremento del registro BP y la posterior decrementación de BX, como contador de iteraciones.

Finalmente el salto que genera el loop, hasta que BX valga cero.

Plantearé otros ejemplos de la visión de engines de mutación y polimorfismo. Por ejemplo, en la red podemos encontrar las variantes posibles para las instrucciones en ensamblador: (ver Listado 1)

>>> Listado 1

```
primer byte
        operador
       /    \
  7 6 5 4 3 2 1 0
  0 0 |       0 | |
      |         | 1 = 16 bit
      |         | 0 = 8 bit
      |         1 =  a reg
      |         0 =  a mem
      |
      0 0 0 = add
      0 0 1 = or
      0 1 0 = adc
      0 1 1 = sbb
      1 0 0 = and
      1 0 1 = sub
      1 1 0 = xor
      1 1 1 = cmp
```

```
segundo byte - modo registro y direcciones
modo dest  origen
/ \ /   \  /  \
7 6 5 4 3 2 1 0
|   |     |
|   |     0 0 0 = [ BX+SI+]
|   |     0 0 1 = [ BX+DI+]
|   |     0 1 0 = [ BP+SI+]
|   |     0 1 1 = [ BP+DI+]
|   |     1 0 0 = [ SI+]
|   |     1 0 1 = [ DI+]
|   |     1 1 0 = [ BP+]
|   |     1 1 1 = [ BX+]
|   0 0 0 = AX (al)
|   0 0 1 = CX (cl)
|   0 1 0 = DX (dl)
|   0 1 1 = BX (bl)
|   1 0 0 = SP (ah)
|   1 0 1 = BP (ch)
|   1 1 0 = SI (dh)
|   1 1 1 = DI (bh)
0 0 - registros indices solo (menos bp)
Si el indice reg es [ bp+] entonces
0 0 = [ 1000h] la longitud sera de 16 bit
0 1 - inmediato, es de 8 bits
1 0 - inmediato, es de 16 bits
1 1 registro a registro
    los bits origen, son segundos
registros usando la misma codificación
como destino.
```

Como podemos ver, la codificación de instrucciones no es tan compleja como parece, y analizando las opciones que tenemos podemos comprender como una engine de mutación o polimorfismo desensambla, configura, y permuta las instrucciones.

En el número anterior vimos un ejemplo de un trocito de código, donde se ha utilizado polimorfismo para deformarlo:

```
mov  ax, 808h
```

Esa instrucción de allí arriba, podemos convertirla en algo como:

```
mov  ax, 303h ; ax = 303h
mov  bx, 101h ; bx = 101h
add  ax, bx   ; ax = 404h
shl  ax, 1          ; ax =
808h
```

Siempre estamos hablando de que la metodología de RX depende de muchos factores, uno de ellos, como se expone, es la suerte.... el algoritmo tiene que tener un error o debería estar mal diseñado o poseer errores en el diseño.

¿por qué pasaría esto?, simplemente, porque los desarrolladores de virus, generalmente son amateurs en el diseño de algoritmos criptográficos.

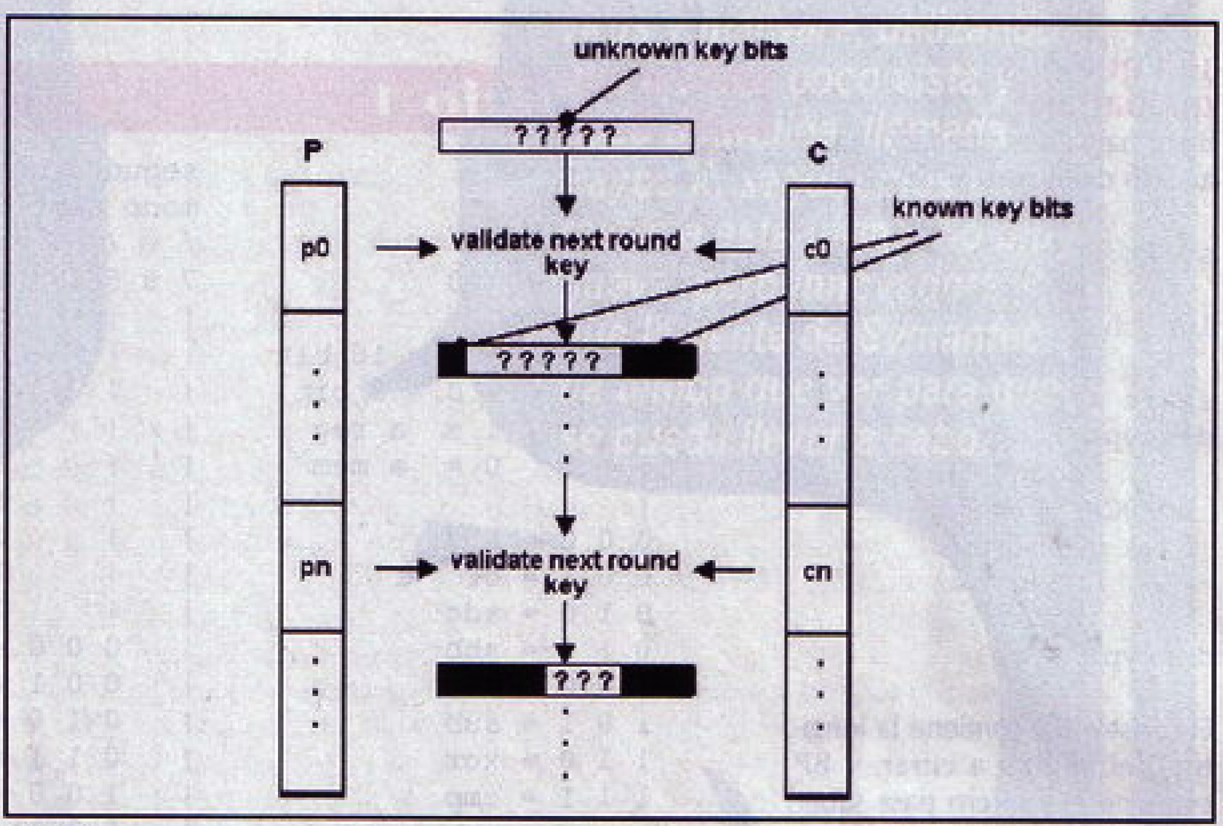
Debemos entender también, que el método de RX, no reemplaza a la emulación.... solo acelera ciertas partes del

proceso, donde se vé involucrado un proceso criptográfico.

La emulación de código, es utilizada en muchas situaciones importantes, a la hora del análisis vírico.Sin embargo, hay momentos o situaciones en donde la emulación, no es recomendable.

Por ejemplo, cuando los virus utilizan RDA (Random Decoding Algorithms). Estos virus, contienen algoritmos de fuerza bruta que son utilizados, para obtener la clave para desencriptarse a sí mismos, ya que no poseen la clave, al haber sido cifrados con una clave aleatoria.

Si estos algoritmos de cifrado fueran emulados, sería muy costoso, para el scanner, es ahí donde los RX entran en acción, y hacen esto posible.



Bagif-RX

El método de los RX en la práctica

La importancia de la geometría

Le llamamos "geometría" a las posiciones y los tamaños de los segmentos que caracterizan a los objetos infectados, como por ejemplo la posición del decriptor del virus, y el cuerpo del mismo.

Así como también los tamaños máximos y mínimos del decriptor, el tamaño del archivo más chico infectado, etc.

En la métodología de los RX, se recomienda elegir apropiadamente los rangos en los que debe ser aplicada, ya que sino pueden obtenerse problemas en el rendimiento del sistema.

Igualmente tenemos un problema muy grande en éste método, es que, es muy dependiente del virus que se esté analizando, ya que como mencioné en el párrafo anterior, sino tendremos problemas de rendimiento.

¿Por qué pasa esto?, porque los virus pueden aparecer al final del fichero, al principio, al final de la sección de datos, al principio, etc.

Por ejemplo, las familias de virus W32/Bagif y W95/Perenast ubican su decriptor cerca del final de la primera sección de los ejecutables, y ubican el virus encriptado en el final de la última sección.

Podemos aplicar RX al final de cada sección de cada fichero, es una posibilidad de encontrar los virus, pero obviamente no encontraremos todos los virus ahí. :)

También podemos observar las características de los infectados y compararlas con las de los demás y encontrar un conjunto de infectados, reduciendo así las iteraciones y no haciendo tan costoso el escaneo... pero eso no es el problema central.

Otro tipo de filtro utilizado, es calcular el radio de bytes que son equivalentes a cero, contra los que no son cero. Si la cuenta excede en bytes iguales a cero, entonces seguramente no se encuentre el cuerpo del virus en ese lugar del archivo.

Entonces, podríamos extender este pensamiento a tratar de ubicar los bytes más "aleatorios" posibles, y así poder "deducir" que se tráta del cuerpo cifrado de nuestro buscado virus.

Esto lo podemos llevar a cabo graficando un histograma de frecuencias.

La familia de virus Efish también ubican su cuerpo en algñun lugar del final de la sección de código de los ficheros infectados.

La ubicación del cuerpo depende de la estructura del fichero infectado (host). Específicamente, si la tabla de la realocación está presente en la última sección, entonces Efish se moverá abajo de la tabla, para formar un espacio en donde el virus se copiará a sí mismo.

Por último se genera una tabla de sustitución para cifrar, que es aleatoriamente ubicado antes del cuerpo del virus. Luego el virus agrega datos aleatorios entre el cuerpo y la tabla generada, estos datos son aleatorios también.

Entonces, la técnica a seguir, es obtener datos en la cabecera del ejecutable, donde se

incluye el tamaño de la sección de datos. Dos de las tablas (recursos y realocación) requieren, que el tamaño sea correcto y coincidentemente los datos aparecen al final de los archivos, cuando estos están presentes.

Otros virus incluídos son W32/MTX, W32/Simile y W32/Perenast. Aquí se puede aplicar la técnica definida anteriormente, donde se analizan los bytes con cero, contra los que no son cero, pudiendo así determinar si el virus está presente o no.

Un caso práctico W95/Perenast

Esta familia de virus, usan un decriptor polimórfico complejo, donde la variante de cada generación es impredecible prácticamente, aunque el decriptor en sí, termina utilizando un método criptográfico muy débil.

Más que nada desde el punto de vista de implementación y utilización del mismo.

Entonces podemos aplicar RX, sin necesidad de analizar el decriptor. El virus cifra cada dword del cuerpo del virus, XOReándolo con una clave. En cada vuelta, el valor encriptado, es agregado a la clave anterior para generar la nueva clave.

Otras variantes del virus, hacían una rotación de la clave, rotando en 1 la clave, y otras variantes rotan en 2 la clave.

Una rutina de RX, conseguiría el valor inicial de la clave del cuerpo del virus, simplemente XOReando los dos primeros dwords, del virus cifrado, con el del virus descifrado, y computando la diferencia.

Luego puede seguir el proceso, desencriptando el resto del virus cifrado, chequeando en cada paso, que el texto plano concuerda con lo esperado, ésto se hace aplicando las búsquedas por patrones al mismo tiempo. :)

Atacando la capa más debil del virus W32/Bagif

Cuando los virus utilizan varias capas de cifrado, cada capa generalmente cifra el decriptor de la siguiente capa y el cuerpo del virus. Los autores de los virus piensan, que encriptar varias veces el cuerpo de un virus puede ser difícil de hacer RX. Este es el caso de Bagif.

En un análisis más profundo, se encontró una falla en su "caparazón".

Esta familia de virus, utilizan dos capas de cifrado. La primera capa es un decriptor polimórfico que construye la segunda capa que contiene el otro decriptor.

Esta primera capa, es extremadamente compleja, y no se puede ser aplicado RX, sin embargo la segunda capa, es muy simple y el algoritmo es constante. La falla en la implementación permite que al cuerpo del virus se le pueda aplicar RX, sin ninguna referencia del decriptor.

31	41	59	26	53	58	97							07		
27	18	28	1b	2c	46										
7e	e4	c0	de												
						05					fd				
	09								02						
												fa			
												ff			
						01						08			
fe															
			fc												
								fb						03	
			04		06										
											0a				

Tabla de sustitucion de EFISH

Conclusión

Bueno amigos, hemos entrado en terreno teórico, describiendo aspectos prácticos, de familias de virus conocidos y no tan conocidos en el mundo de la informática.

Como podemos ver, el método RX, nos permite muchas variadas técnicas y mezclas a la hora de análisis vírico. Podemos utilizar este tipo de métodos en comunicaciones cifradas, donde sepamos que algoritmos simples son utilizados para cifrar estas comunicaciones... o quizás en un futuro, podamos aplicarlo a algoritmos complejos. :) Espero que les haya gustado. Nos vemos en el próximo número.

SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com

Tras haber estudiado exhaustivamente la unidad de ejecución y la unidad de control, ha llegado el momento de hablar del tercer elemento que describe la arquitectura Von Neumann (o más correctamente, de Eckert-Mauchl): la memoria. Aunque inicialmente fue descrita como un único elemento, los computadores modernos disponen de una compleja jerarquía con un amplio abanico de sistemas de memoria, con el fin de mejorar el rendimiento. Pero, ¿qué tipos de memoria hay? ¿cómo funciona la memoria?

Arquitectura de computadores

Memoria (I)





Sed todos bienvenidos, queridos lectores, a una nueva entrega del curso de arquitectura de computadores. El mes pasado estudiamos una implementación alternativa al método de la tabla de estados para nuestra unidad de control, concretamente el método de las células de retardo. Mediante este método, nos servíamos de una serie de circuitos biestables para propagar la señal de control por el sistema, atendiendo a la función de propagación que nosotros diseñamos. Gracias al circuito iniciador, evitamos las fluctuaciones asociadas a este tipo de componentes electrónicos.

Con dicha práctica dimos por finalizado el estudio de la unidad de control al nivel que deseamos obtener para el presente curso, pues si bien existen otros sistemas de diseño (como las unidades de control microprogramadas), su complejidad haría su estudio excesivamente farragoso. Así pues, comenzamos en esta entrega un nuevo bloque, dedicado a la memoria.

La memoria

En la arquitectura de Eckert-Mauchl (injustamente atribuida a Von Neumann) existe un tercer elemento que, junto a la unidad de ejecución y la unidad de control, conforma el núcleo de proceso del sistema. Este elemento es la unidad de memoria, y su vital importancia estriba en la finalidad de la misma, pues es la encargada de contener todos los datos del sistema.

Un programa está definido por las instrucciones de código máquina que lo componen. Dichas instrucciones son ejecutadas en el procesador -unidad de ejecución- y secuencian las señales de control -en la unidad de control- que gobernarán los estados de la máquina durante el tiempo de ejecución de las mismas. Podríamos decir que son las encargadas de que el sistema siga funcionando. Pues bien, por definición un computador únicamente puede ejecutar instrucciones que se encuentren en memoria.

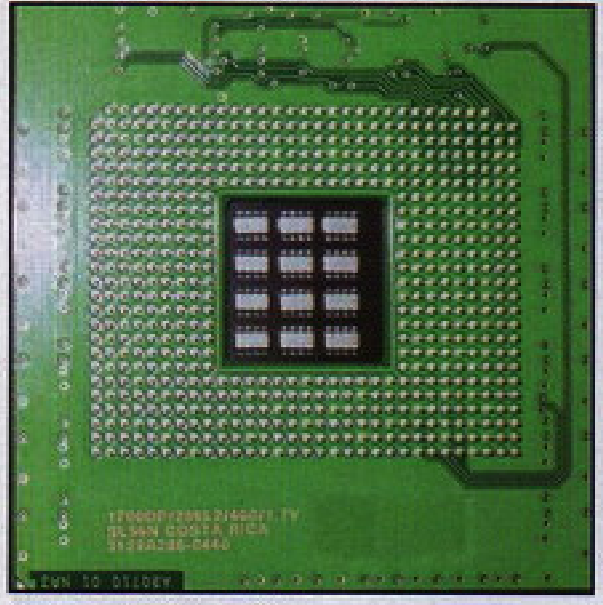
Además, obviamente, todos los datos de entrada que puedan ser leídos durante la ejecución de un programa arbitrario, así como los datos de salida que se generen durante la ejecución del mismo, deben residir en memoria obligatoriamente. Una vez terminada la ejecución del programa, aquello que no haya sido almacenado en memoria se "pierde" en el limbo informático.

Pero, como seguramente todos sabréis, hoy en día no existe un único sistema de memoria en un ordenador. Me viene a la cabeza un ejemplo bastante clarificador: cuando alguien "profano" en el mundo de la informática se quiere comprar un nuevo ordenador, suele pedir algo "con mucha memoria" (o, peor aún, "con muchos gigas de ésos"). De forma completamente automática nos surge una pregunta: ¿de qué tipo?

Y la pregunta no es ninguna tontería. Un ordenador que vaya a ser usado para descargar (y almacenar) música y películas de la red, necesitará una gran cantidad de memoria secundaria (disco duro), pero no



Buffer de 16 Mb de un disco duro


Chips de caché de un P4Xeon

demasiada memoria principal (memoria RAM). Sin embargo, un servidor necesitará una enorme cantidad de memoria principal (RAM), pero no necesitará un disco duro demasiado grande (a no ser que se trate de un servidor de ficheros, claro).

Jerarquía de memoria

Así pues, hoy en día los ordenadores poseen un sistema jerárquico de memoria, cuya clasificación podríamos definir de la siguiente forma: desde las más rápidas, pequeñas y caras, hasta las más grandes, lentas y baratas. Y es que coste y velocidad suelen ir de la mano, siendo inversamente proporcionales al tamaño en la mayoría de los casos.

En un primer nivel encontraríamos los registros del microprocesador. Su velocidad de acceso es la más alta posible, pues aunque varíe entre procesadores, siempre es de un único ciclo de reloj. Dado que ningún procesador puede ejecutar algo en un intervalo de tiempo inferior al de su propio ciclo -es su cuanto de tiempo-, no existe ninguna memoria más rápida que los registros.

El número de registros disponible varía según la arquitectura, pero para que os hagáis una idea, los procesadores "normales" tienen entre 16 y 32 registros en total (la mitad de entero y la otra mitad de punto flotante) de tamaño palabra (32 ó 64 bits, según arquitectura). Es decir, en el mejor de los casos estaríamos hablando de unos 2048 bits de memoria. Ya sabemos que es muy rápida, ya sabemos que es muy pequeña, pero ¿cómo es de cara? Pues, habida cuenta de que está integrada en el circuito del propio microprocesador, muy barata no es...

Memorias caché

En un segundo nivel encontraríamos la memoria caché de primer nivel, que suele separarse en dos grupos: uno para datos y otro para instrucciones. Su velocidad de acceso sigue siendo muy alta, normalmente de uno o dos ciclos del procesador. Su tamaño es algo más grande, siendo lo habitual 32 kb por cada uno de los dos grupos de caché.

En el tercer nivel tenemos la caché de segundo nivel, que ya tiene unificados los datos y las instrucciones. La velocidad de acceso comienza a verse resentida, girando en torno a los diez ciclos de procesador, siendo ya mucho más lenta que la caché de primer nivel. El tamaño de esta caché depende absolutamente de la arquitectura, pues donde la caché de primer nivel no ha variado prácticamente con el paso de los años, la de segundo nivel es la que se está aumentando cada vez más en aras del rendimiento. Desde los 512 kb del Pentium II, hasta los 8 Mb del Core 2 Quad, la variedad de tamaños -y, ojo, velocidad- de estas cachés es muy grande.

Ambas cachés son muy caras de aumentar, pues hoy en día se encuentran integradas dentro del encapsulado del propio microprocesador. De hecho, ocupan la mayor parte del área de silicio del mismo, y además acarrean problemas colaterales

>>> Listado 1

```
00      EMPEZAR
01              VARIABLE VECTOR(8) ENTERO mivector
02              inicializar(mivector)
03              DESDE i=1 HASTA i=8
04                      mivector(i) <= i * 100
05              FIN DESDE
06              DESDE i=1 HASTA i=8
07                      imprimir(mivector(i))
08              FIN DESDE
09      TERMINAR
```

>>> Listado 2

```
00      EMPEZAR
01              VARIABLE VECTOR(8) ENTERO mivector
02              VARIABLE ENTERO temporal
03              inicializar(mivector)
04              DESDE i=1 HASTA i=8
05                      adquirir(temporal)
06                      procesar(temporal)
07                      mivector(i) <= temporal
08              FIN DESDE
09      TERMINAR
```

>>> Listado 3

```
//
// Código extraido de http://www.cs.utk.edu/~mucci/cache-
bench
//
do i=1, max_length
        start_time
        do j=1, max_iterations
                do k=1, i
                        A(k)=i
                enddo
        enddo
        stop_time_and_print
enddo
```

como el aumento de la potencia disipada en forma de calor, que conlleva el siempre problemático asunto de la temperatura.

Estas memorias de tipo caché son las principales responsables del aumento de rendimiento en la actualidad, en lo que a cuestiones de memoria se refiere. Esto es debido, principalmente, a que son capaces de aprovechar los denominados principios de localidad espacial y temporal en las referencias a memoria. Veamos qué significan estos términos con un poco más de detalle...

Localidad espacial y temporal

La localidad espacial nos dice que, dado un acceso a un elemento arbitrario de memoria, es muy probable que en un intervalo corto de tiempo se acceda a una posición contigua. Esto es debido a factores como la secuencialidad de las instrucciones de un programa, o a la linealidad de las estructuras de datos de tipo vector. Echemos un vistazo al siguiente código: (ver Listado 1)

Debido a la estructura intrínseca del programa, todas las instrucciones se ejecutan en secuencia, por lo que si cuando carguemos la instrucción inicial "00" en memoria llevamos igualmente a caché las dos o tres siguientes, el tiempo de acceso a dichas instrucciones se verá enormemente reducido, pues no será necesario ir a "buscarlas" a memoria principal.

De igual forma, la variable de tipo vector "mivector" es utilizada siempre de forma lineal, accediendo a sus elementos de forma ordenada y secuencial. Así, en el bucle de impresión, si cuando iteramos por primera vez y cargamos el primer elemento del vector, aprovechamos para trasladar a memoria caché los siete elementos siguientes, las siguientes iteraciones serán mucho más rápidas al no tener que leer de la memoria principal cada vez.

La localidad temporal supone que, dado un acceso a un elemento arbitrario de memoria, es muy probable que dicho elemento sea accedido nuevamente en un intervalo corto de tiempo. Factores como la repetición de iteraciones en bucles, o la utilización de datos tras su cómputo, avalan esta tesis. Echemos un vistazo al siguiente código: (ver Listado 2)

Podemos observar que el bucle está compuesto de tres instrucciones ("05", "06" y "07") que se repetirán ocho veces, tantas como iteraciones tiene dicho bucle. Si estas instrucciones permanecen en memoria caché durante el tiempo que tarda en ejecutarse el bucle, no será necesario cargarlas una y otra vez, con la pérdida de ciclos de proceso que supone el acceso a memoria principal.

Por otro lado, podemos ver cómo ciertos datos son utilizados inmediatamente después de haber sido calculados, como el caso de la variable "temporal": primero se usa para escribir en ella el valor adquirido y después se procesa, para finalmente almacenarse en el vector. Si cada vez que se utiliza la variable hubiera que cargarla de memoria principal, operar sobre ella y escribir nuevamente, la pérdida de ciclos sería enorme. En lugar de eso, la variable es cargada en caché, y se trabaja en dicha zona de memoria, para escribir en memoria principal únicamente cuando no va a ser utilizada más. Realmente, esto último no es exactamente así, pues deben definirse ciertas políticas con respecto a la caché para saber qué hacer cuando un dato de la misma es modificado. Pero eso es algo de lo que hablaremos en otro momento.

Aprovechando la caché

El uso de la memoria caché no se reduce



únicamente a un aumento de rendimiento circunstancial que queda a la mano del hardware, sino que puede ir mucho más allá. Por ejemplo, existe un programa de pruebas de rendimiento para unidades de punto flotante de microprocesadores llamado Whetstone que, gracias a que cabe completamente en la caché del microprocesador, permite eliminar la influencia del acoplamientro entre memoria y procesador, obteniendo así resultados más fiables.

El código fuente de Whetstone -en lenguaje de programación Pascal- puede ser encontrado en el siguiente enlace a la Wikipedia: http://es.wikipedia.org/wiki/Whetstone

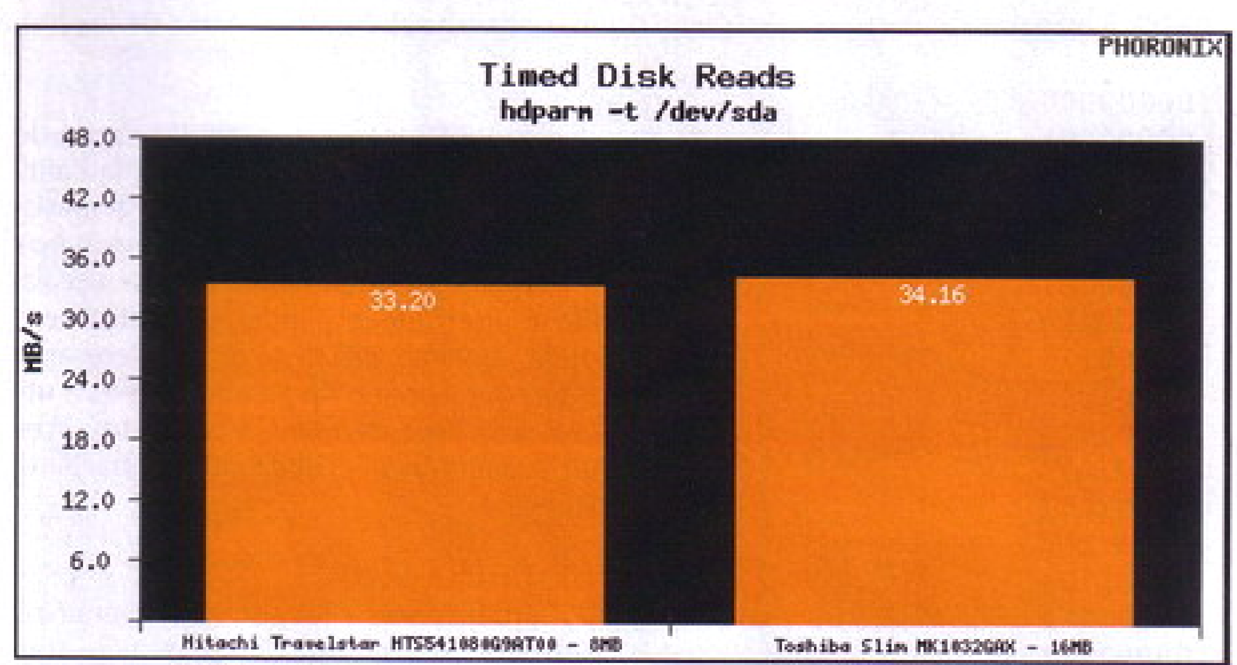
Un sencillo programa que podría actuar como benchmark de memoria caché es el descrito por el siguiente pseudocódigo: (ver Listado 3)

Memoria secundaria

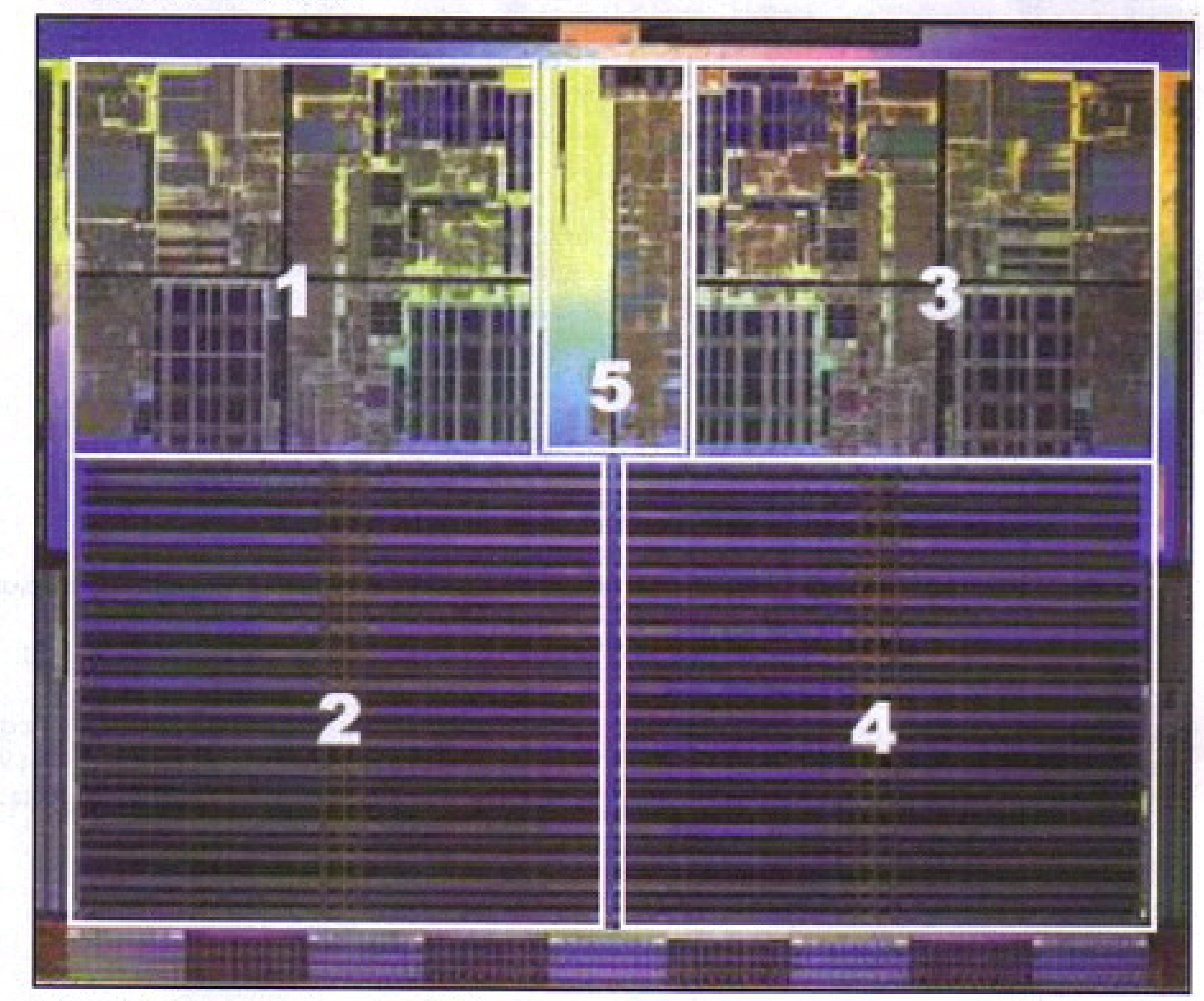
Los sistemas de memoria de los que hemos hablado anteriormente se encuentran todos a un nivel inferior a la memoria principal. Los registros son elementos prácticamente indispensables para el correcto funcionamiento de las rutas de cómputo del microprocesador, pero las cachés podríamos considerarlas unos apoyos al sistema de memoria principal. En concreto, se trata de un apoyo al rendimiento, logrando memorias más rápidas y más "cercanas" al nivel de trabajo del procesador.

Pero existe otro tipo distinto de apoyo a la memoria, con dos objetivos principalmente: hacerla persistente y aumentar su tamaño. Lo primero es debido a que las memorias utilizadas en los ordenadores actuales son volátiles, esto es, necesitan ser constantemente alimentadas con corriente para "refrescar" su información y poder mantener los datos almacenados. Cuando un ordenador se apaga, o cuando hay una pérdida de fluido eléctrico (benditos SAI), toda la información que haya en la memoria RAM irá a parar, nuevamente, al "limbo".

Por otro lado, y aunque la cantidad de RAM instalada en los ordenadores actuales ha experimentado un crecimiento muy elevado, sigue siendo manifiestamente insuficiente para almacenar todos los datos que maneja un usuario hoy en día. Lo actualmente en día son 2 ó 4 Gb de memoria RAM, y de hecho los sistemas operativos de 32 bits tienen problemas para direccionar más de 4 Gb de memoria; mientras que la instalación de un Windows XP o un Linux supone, respectivamente, unos 8 y 5 Gb de espacio.



Comparación de cachés de disco



La mitad del área es ocupada por la caché L2

Así pues, es necesario disponer de un almacenamiento masivo que sea capaz de contener una gran cantidad de información de forma persistente. Los encargados de dicha tarea son los discos duros, que hoy en día se mueven en el rango del terabyte de información. Y parece que el futuro pasa por los discos duros de estado sólido (SSD), basados en la misma tecnología que las tarjetas de memoria o los socorridos "pen drive".

Memoria principal

Y llegamos por fin a la memoria principal, la más importante dentro de la jerarquía, pues no obstante ya hemos visto que el resto de niveles tienen como único fin apoyar a éste. La manifestación actual de la memoria principal en nuestros ordenadores es la archiconocida memoria RAM.

El acrónimo RAM (Random Access Memory) nos indica que se trata de una memoria de acceso aleatorio, es decir, que el tiempo de acceso a cada posición es constante, e independiente de la situación física de dicho elemento de almacena-

>>> Listado 4

```
00000000
00000001
00000010
00000011
00000100
00000101
00000110
00000111
00001000
00001001
00001010
00001011
00001100
00001101
00001110
00001111
00010000
00010001
00010010
00010011
00010100
00010101
00010110
00010111
00011000
00011001
00011010
00011011
00011100
00011101
00011110
00011111
```

miento de memoria. Es la contraposición a las memorias de acceso secuencial, como las unidades de cinta, los discos compactos, o los discos duros magnéticos tradicionales; en los que cuando se solicitan dos datos que se encuentran físicamente muy alejados entre sí, es necesario realizar un desplazamiento físico de la cabeza lectora. Las memorias RAM, así como las memorias flash o los discos de estado sólido, no necesitan realizar ningún desplazamiento físico, siendo todos los direccionamientos puramente electrónicos.

Las memorias RAM actuales se encuentran en forma de módulos, bien sean SIMM (ya anticuados), DIMM (los más utilizados) o RIMM (que nunca llegaron a triunfar). El tamaño es también variable, siendo hoy en día el estándar 512 ó 1024 Mb por módulo, y existiendo módulos mayores según el ámbito de aplicación. Las frecuencias de trabajo se han visto incrementadas en los últimos años, pasando de los 66-100-133 MHz de las memorias SDRAM a los hoy en día habituales 800 MHz de las memorias DDR2. Y existen memorias de frecuencias aún más altas, hasta los 1600 MHz de los módulos PC3-12800 de DDR3.

Pero, si nos metemos ya en el terreno de la arquitectura de computadores, la cantidad de memoria no es un tema demasiado interesante. Simplemente, nos encargamos de que sea fácilmente escalable y direccionable independientemente de la cantidad utilizada. Sí es interesante saber qué tamaño de palabra vamos a utilizar a la hora de manejar los datos, y es un aspecto al que dedicaremos bastante atención.

Memoria virtual

Los ordenadores y los sistemas operativos actuales, aún cuando disponen de una cantidad muy elevada de recursos, a veces pueden verse saturados por el consumo de los procesos en ejecución. Parafraseando a Blade Runner, yo he visto cosas que vosotros no creeríais: procesos Java que consumen casi un giga y medio de memoria RAM para mapear una ontología en memoria, análisis de sintaxis para generación de bases de datos que tardan en ejecutarse casi una hora en un servidor con dos procesadores de cuatro núcleos cada uno...

Para esos momentos en que la demanda de recursos puede resultar excesiva, el sistema operativo se guarda un as en la manga: hacer creer a sus procesos que posee recursos casi ilimitados. En el caso de la memoria, este truco se logra mediante la llamada memoria virtual. Así, cuando la cantidad de memoria libre en el ordenador baja por debajo de un determinado nivel que puede considerarse inaceptable, el sistema operativo comienza a "expulsar" ciertos datos de la memoria principal, guardándolos en el disco duro hasta el momento en que vuelvan a ser necesarios, cuando los rescatará y volverá a colocar en memoria principal. El truco es que el proceso no sabe que esto ocurre, por lo que piensa que está ocupando tanta memoria como solicite.

Modelando una memoria ROM

Una memoria ROM, al contrario que los tipos de memoria de los que hemos esta-

>>> Listado 5

```
USE STD.textio.all;

PACKAGE file_pack IS

      --tipo de datos par auna memoria ROM de n posicio-
nes de 8 bits
      TYPE memoria_nx8 IS ARRAY(INTEGER RANGE<>) OF
BIT_VECTOR(7 DOWNTO 0);
      --procedimiento de carga de la memoria ROM
      PROCEDURE cargar_rom(VARIABLE palabra:INOUT memo-
ria_nx8; VARIABLE fichero_rom: IN text);

END file_pack;

PACKAGE BODY file_pack IS

      --procedimiento de carga de la memoria ROM
      PROCEDURE cargar_rom(VARIABLE palabra:INOUT memo-
ria_nx8; VARIABLE fichero_rom: IN text) IS

      VARIABLE L:line;
      VARIABLE i:integer;

      BEGIN
            FOR i IN palabra'RANGE
            LOOP
                        readline(fichero_rom,L);
                        read(L,palabra(i));
            END LOOP;
      END cargar_rom;

END file_pack;
```



do hablando hasta ahora, contiene datos que únicamente pueden ser leídos, esto eso, se trata de una memoria de sólo lectura (Read Only Memory). Por tanto, puede ser utilizada como fuente de obtención de datos o de instrucciones de código máquina, pero nunca podremos almacenar en ella resultados.

Para familiarizarnos con el trabajo con elementos de memoria en VHDL, la primera práctica que vamos a realizar consistirá en, utilizando un fichero que contendrá información de sólo lectura (que simulará el comportamiento de una memoria ROM), modelar el proceso de adquisición de datos, teniendo en cuenta la dirección especificada por el bus de direcciones así como las señales de control pertinentes, para volcar la información a un bus de datos como el que hemos venido utilizando los últimos meses.

Este proceso es también parte fundamental del ciclo de ejecución de un computador, pues cada vez que se carga una instrucción de código máquina en la unidad de control, y cada vez que se desea obtener un dato para realizar un cómputo, deben obtenerse dichos fragmentos de información de una memoria. El proceso siempre es el mismo: especificar la dirección a leer (o escribir), activar las señales de control adecuadas, y por último leer del bus de datos la información que ha sido volcada a él por el controlador pertinente.

Vamos a simular una unidad de memoria ROM de 32 posiciones de ancho de palabra de 8 bits, mediante un fichero de texto que contendrá la siguiente información: (ver Listado 4)

Si alguien se anima, estaría bien que intentarais, con los conocimientos de que ya disponéis, realizar un programa en VHDL que simule el comportamiento que he descrito en los anteriores párrafos.

Eso sí, para poder cargar la ROM necesitaremos trabajar con ficheros de texto en VHDL, algo que no hemos necesitado hacer hasta ahora. Por ello, vamos a crear un nuevo paquete de código que se encargue de estos menesteres, y cuyo código es el siguiente: (ver Listado 5)

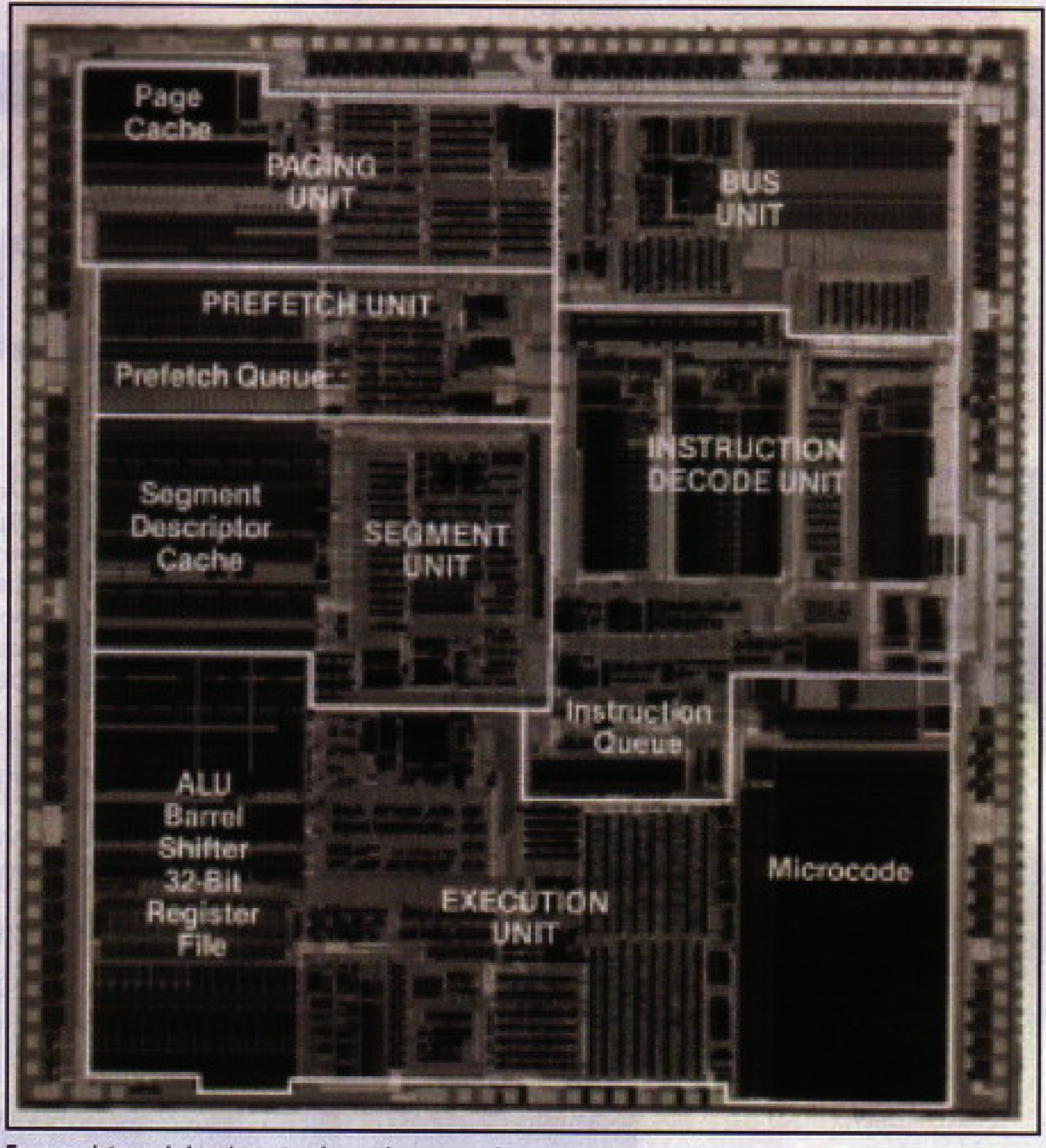
No hace falta dar demasiadas explicaciones sobre su funcionamiento, aunque el mes que viene veremos cómo utilizarlo en la implementación que dejamos indicada.

El mes que viene

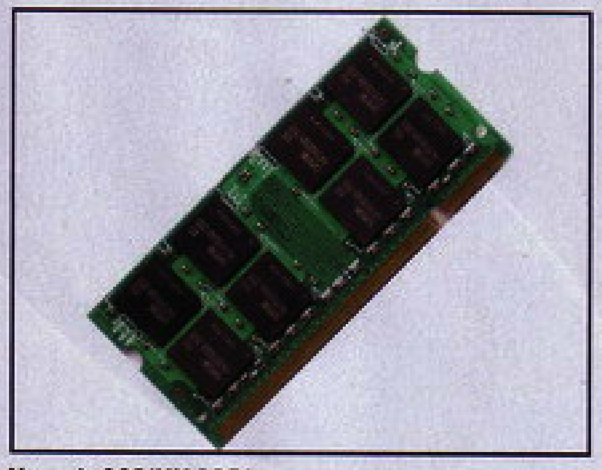
Este mes ha estado compuesto prácticamente de forma completa por teoría sobre el sistema de memoria de un computador. Puede resultar pesado, y sé que es mucho más divertido trastear con el código y el simulador, pero para comprender bien el funcionamiento de los elementos con los que trabajaremos más adelante, resulta necesario tener una cierta base teórica.

Aún así, creo que toda esta teoría habrá resultado interesante a todos aquellos que gusten de cacharrear con sus ordenadores, y de hecho posiblemente muchos de vosotros ya estaríais al tanto de la mayoría de los aspectos que he comentado. El mes que viene seguiremos justo donde lo hemos dejado, trabajando con nuestra unidad de memoria ROM.

Hasta que ese momento llegue, disfrutad. ¡Nos leemos!



Esquema interno de los elementos de un microprocesador



Memoria SODIMM DDR2



Disco duro de estado sólido

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com<

Parte VI

Criptografía asimétrica

Hoy les traigo un complemento del número anterior, en el cuál veremos más de cerca las alternativas que tenemos con la CCE (Criptografía de curvas elípticas), además de utilizar una librería GPL, para implementar ejemplos.

Número anterior

En el número anterior vimos solamente ESDSA, que es utilizado para firmar documentos y verificar las firmas... pero como veremos hoy, podemos utilizar CCE, de otras muchas formas más.

Luego vimos los pasos de generación de claves, y verificación. Como nuestros amigos Alice y Bob realizan todo el proceso. Finalmente terminamos el artículo con OpenSSL, el cuál implementa CCE.

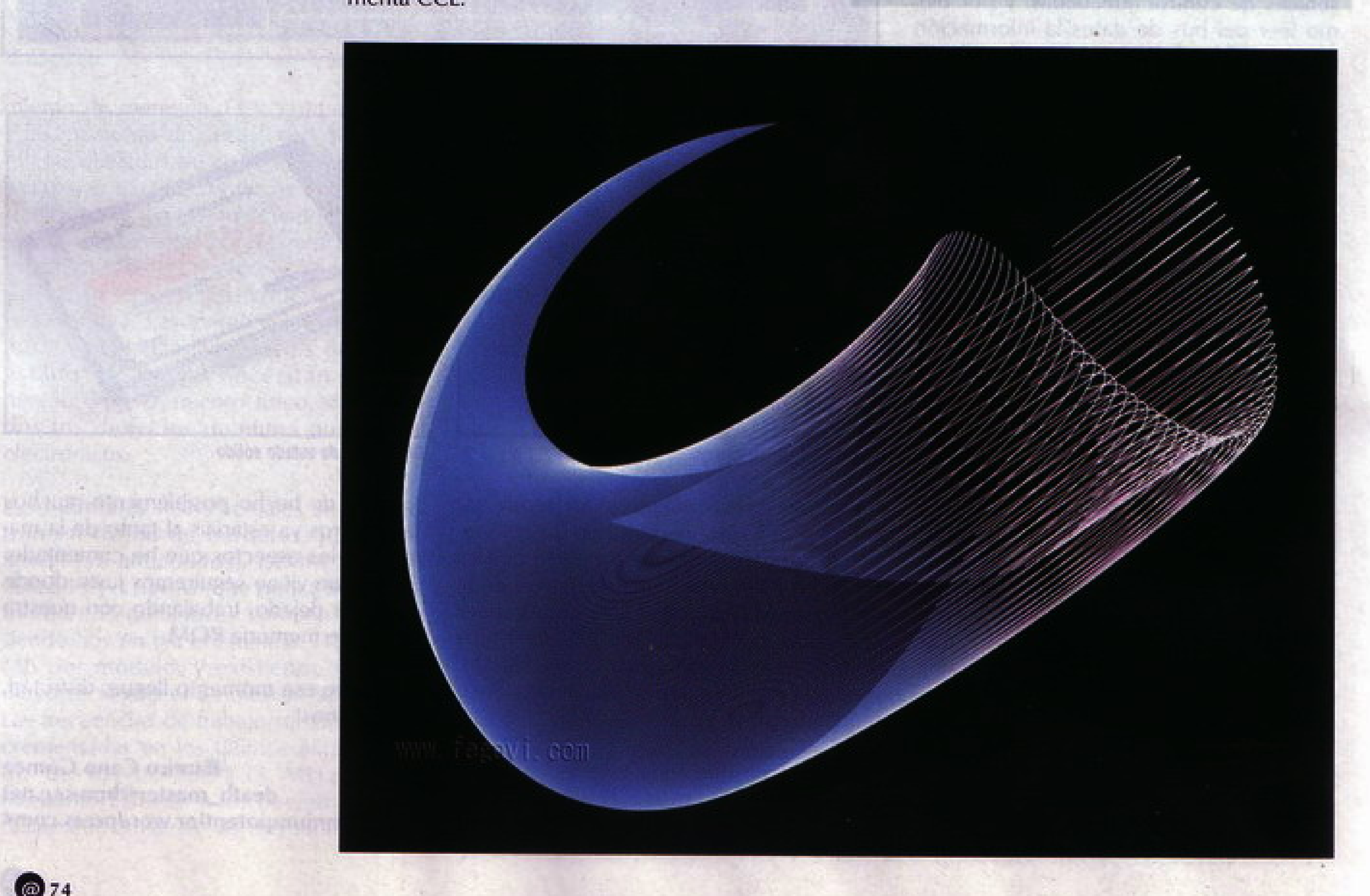
Desde la versión 0.9.8 la herramienta OpenSSL ofrece algunas opciones para trabajar con curvas elípticas. No están muy documentadas, pero nos servirán para realizar una pequeña demostración del uso de la firma digital.Para generar un clave ejecutaremos el siguiente comando:

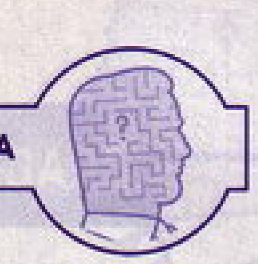
```
$ openssl ecparam -genkey -name
secp224r1 -out key.pem
```

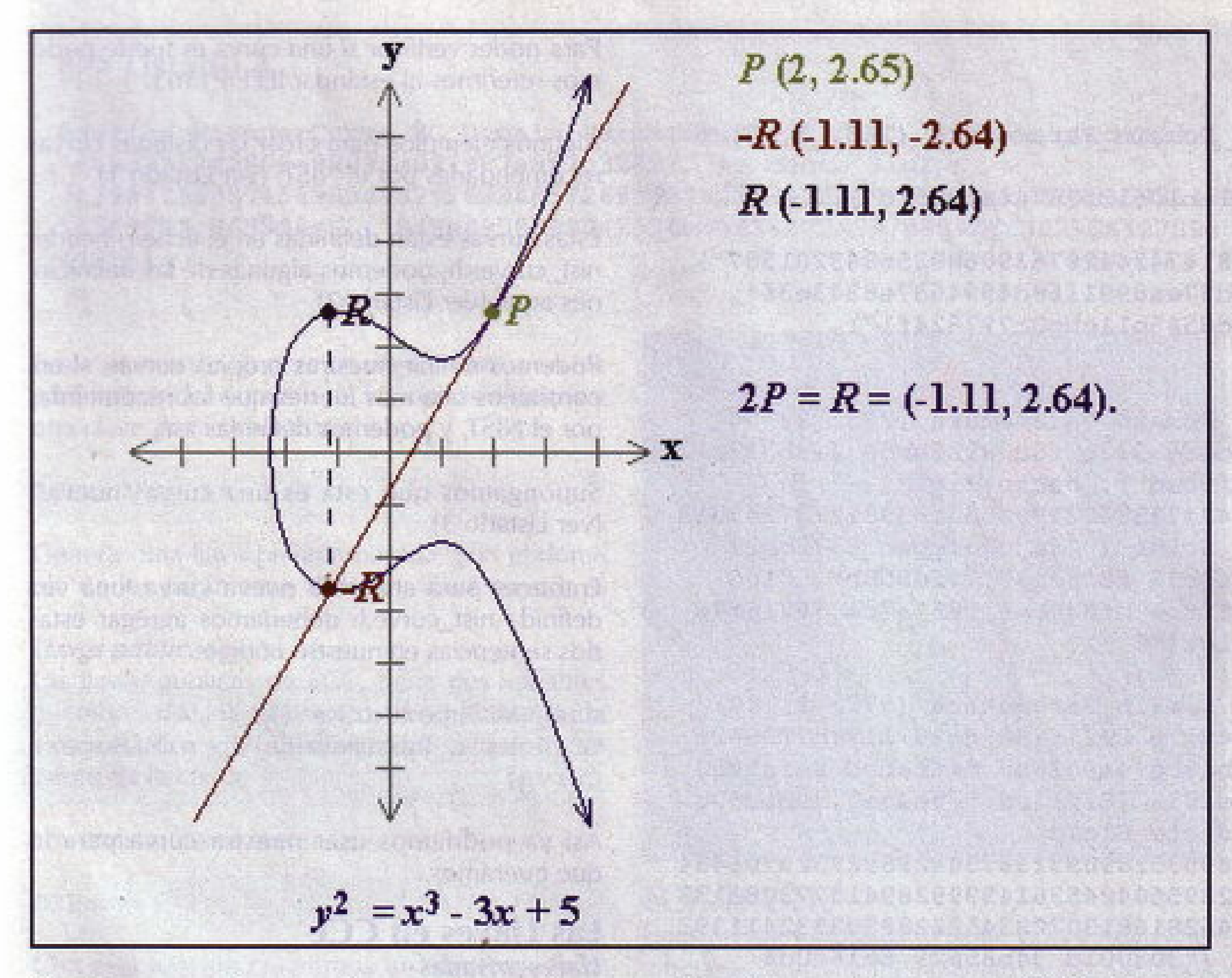
Ahora tanto la clave pública como la privada se encuentran dentro de key.pem.

Podemos extraer la pública con el comando:

```
$ openssl ec -in key.pem -text -
pubout -out pubkey.pem
```







Ya disponemos de una clave con la que hacer pruebas, por lo que generaremos un mensaje que firmar:

```
$ echo "El mensaje de prueba de
h4ck1t!" > msg.txt
```

Y lo firmaremos, operación que solo puede realizar el propietario de la clave privada:

```
$  openssl dgst -sign key.pem -
ecdsa-with-SHA1 < msg.txt >
msg.sig
```

Firmado el mensaje, todo usuario que disponga de la clave pública podrá verificar su procedencia:

```
$ openssl dgst -verify pubkey.pem
-ecdsa-with-SHA1 -signature
msg.sig < msg.txt

Verified OK
```

Entrando en profundidad con CCE

La librería que utilizaremos se llama borZoi, y contiene todo lo necesario para implementar cualquier algoritmo que forma parte del esquema de CCE.

Según el NIST, el Instituto Nacional de Ciencia y Tecnología perteneciente a Estados Unidos, hay algunas curvas recomendadas para la utilización eficiente y fuerte en el cifrado de curvas elípticas.

Igualmente recomiendo chequear la fortaleza de estas curvas ustedes solos.... por las dudas ;)... uno nunca sabe porque en realidad recomiendan ESAS curvas... :)

>>> Listado 1

```
Ejemplo de curva NIST_B_163
use_NIST_B_163 ();
EC_Domain_Parameters dp = NIST_B_163;

Ejemplo de curva NIST_B_233
use_NIST_B_233 ();
EC_Domain_Parameters dp = NIST_B_233

Ejemplo de curva NIST_B_283
use_NIST_B_283 ();
EC_Domain_Parameters dp = NIST_B_283;

Ejemplo de curva NIST_B_409
use_NIST_B_409 ();
EC_Domain_Parameters dp = NIST_B_409;

Ejemplo de curva NIST_B_571
use_NIST_B_571 ();
EC_Domain_Parameters dp = NIST_B_571;
```

>>> Listado 2

```
#define NIST_B_163 EC_Domain_Parameters (163, 3, 7, 6,
3, Curve ("1",
"20a601907b8c953ca1481eb10512f78744a3205fd"),
decto_BigInt
("5846006549323611672814742442876390689256843201587"),
Point ("3f0eba16286a2d57ea0991168d4994637e8343e36",
"0d51fbc6c71a0094fa2cdd545b11c5c0c797324f1"),
decto_BigInt ("2"));

#define NIST_B_233 EC_Domain_Parameters (233, 2, 74,
Curve ("1", "066 647ede6c 332c7f8c 0923bb58 213b333b
20e9ce42 81fe115f 7d8f90ad"), decto_BigInt
("6901746346790563787434755862277025555839812737345013
555379383634485463"), Point ("0fa c9dfcbac 8313bb21
39f1bb75 5fef65bc 391f8b36 f8f8eb73 71fd558b", "100
6a08a419 03350678 e58528be bf8a0bef f867a7ca 36716f7e
01f81052"), decto_BigInt("2"));

#define NIST_B_571 EC_Domain_Parameters (571, 3, 10,
5, 2, Curve ("1", "2f40e7e 2221f295 de297117 b7f3d62f
5c6a97ff cb8ceff1 cd6ba8ce 4a9a18ad 84ffabbd 8efa5933
2be7ad67 56a66e29 4afd185a 78ff12aa 520e4de7 39baca0c
7ffeff7f 2955727a"), decto_BigInt
("3864537523017258344695351890931987344298927329706434
9986572352514515191422895604245361439993894157730831333
8811219269444862468724628168130702345282883033324113933
191105285703"), Point ("303001d 34b85629 6c16c0d4
0d3cd775 0a93d1d2 955fa80a a5f40fc8 db7b2abd bde53950
f4c0d293 cdd711a3 5b67fb14 99ae6003 8614f139 4abfa3b4
c850d927 e1e7769c 8eec2d19", "37bf273 42da639b 6dccff-
fe b73d69d7 8c6c27a6 009cbbca 1980f853 3921e8a6
84423e43 bab08a57 6291af8f 461bb2a8 b3531d2f 0485c19b
16e2f151 6e23dd3c 1a4827af 1b8ac15b"), decto_BigInt
("2"));
```

Para poder verificar si una curva es fuerte podemos referirnos al estándar IEEE P1363.

Algunos ejemplos para crear las distintas curvas recomendadas por el NIST: (ver Listado 1)

Estas curvas están definidas en el fichero header nist_curves.h, podemos algunas de las definiciones aquí: (ver Listado 2)

Podemos definir nuestras propias curvas, si encontramos una más fuertes que las recomendas por el NIST, y podemos definirlas así:

Supongamos que esta es una curva "nueva". (ver Listado 3)

Entonces para aregar la nueva curva, una vez definida nist_curve.h deberíamos agregar estas dos sentencias en nuestro código:

```
use_ MiSuperCurva ();
EC_Domain_Parameters dp = MiSuper-
Curva;
```

Así ya podríamos usar nuestra curva para lo que queramos..

Las Llaves en CCE

Llaves privadas

La librería contiene dos miembros privados. Uno es dp, que sería el dominio de los parámetros de las curvas elípticas y la variable s, que se trata de un número entero grande (BigInt), es la clave privada y debe ser mantenida en secreto.

Los constructores son:

```
ECPrivKey (dp);
```

borZoi

borZoi is a C++ Elliptic Curve Cryptography Library which implements the following algorithms using elliptic curves defined over finite fields of characteristic 2 ($GF2^m$):

- ECDSA (Elliptic Curve Digital Signature Algorithm)
  As specified in ANSI X9.62, FIPS 186-2 and IEEE P1363.
- ECIES (Elliptic Curve Integrated Encryption Scheme)
  As specified in ANSI X9.63 and the IEEE P1363a Draft.
- Elliptic Curve Diffie-Hellman Key Agreement Scheme
  As specified in ANSI X9.63 and IEEE P1363.

The AES symmetric encryption scheme (NIST AES draft) and SHA-1 hash algorithm (FIPS 180-1) are also included.

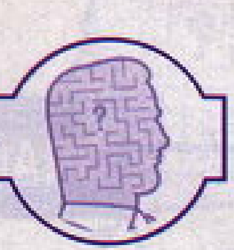
Licensing:

borZoi can be freely downloaded and used under the terms of the GNU GPL. Please contact sales@dragongate-technologies.com for details of commercial licensing options. We welcome any comments or bug reports which you may have, however please note that we cannot accept any patches for legal reasons, because some of the borZoi code is also used in our commercial products.

Documentation:

The draft version of the manual is now available for download below and is also included in the source distribution:

Terminado



>>> Listado 3

```
#define MiSuperCurva EC_Domain_Parameters (233, 7, 1, 2, 6, Curve ("1",
"6aad3232f2898e98098c097987a8f7g328273"), decto_BigInt
("3984759837456983498752639485726934876298347562"), Point ("43a54354375a447654 7654e989
769f7757 865898e", "848a8909d89042534e36338472a347e9842ff36253542789e"), decto_BigInt
("2"));
```

Este constructor, genera un objeto llave, con los parámetros del dominio de las curvas elípticas y una clave privada aleatoria.

```
ECPrivKey (dp, s);
```

Genera una llave privada basada, con el dominio de los parámetros dp y una llave privada s.

Llaves públicas
Las llaves públicas de ECC, tiene dos variables miembro, dp, los parámetros de dominio de la curva elíptica y W, la llave pública que es un punto de la curva.

Los constructores son:

```
ECPubKey ();
```

Con esta función crearemos un objeto de llave pública vacío.

```
ECPubKey (sk);
```

Esta función sirve para crear una llave pública desde una llave privada.

```
ECPubKey (dp, W);
```

Crea una llave pública con los parámetros de dominio dp y la llave pública W.

Los métodos son:

```
valid ();
```

El método valid, devuelve un valor booleano, para determinar si la llave pública es válida o no.

Primer Ejemplo
En este ejemplo, se genera una llave privada usando la curva NIST_B_163 y calculando la llave pública.

```
use_NIST_B_163 ();
EC_Domain_Parameters dp =
NIST_B_163;
ECPrivKey sk (dp); // generamos la
llave privada
ECPubKey pk (sk); // calculamos la
llave pública derivado de la privada
```



ECKAS-DH1
Estas iniciales significan Elliptic Curve Key Agreement Scheme, Diffie-Hellman 1, donde, cada parte combina su clave privada con la llave pública de la otra parte, para calcular una llave secreta compartida, la cuál, puede ser usada, para cifrar de manera simétrica, con un algoritmo como por ejemplo AES.

Otra información es generada también para las dos partes. Puede ser usada como parámetros de derivación para asegurar que una llave secreta es generada por cada sesión.

Este esquema de llaves, está descrito en más detalle en la sección 9.2 del estándar IEEE P1363.

Conclusión
Bien amigos, hemos visto de manera muy detallada cómo utilizar esta librería para iniciarnos en el nuevo mundo de la criptografía asimétrica utilizando curvas elípticas.

En el próximo veremos mas esquemas de llaves y protección, que no suelen analizarse en detalle, con ejemplos prácticos en cada caso.

Nos vemos en el próximo número.

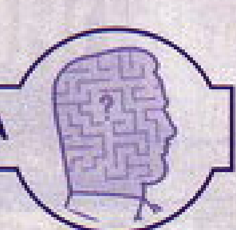
SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com

Criptografía clásica

Cifrador de Hill

En el anterior capítulo se habló sobre los cifradores poligrámicos, en este continuamos con ellos y en especial con el cifrador de Hill, un sistema quizás anticipado a la época en la que se creó y que por falta de medios no pudo competir con la máquina alemana Enigma, aunque finalmente se patentó una maquina de cifrado en 1932. Actualmente con los ordenadores este sistema no posee la mayor complicación de implementación.





Introducción

El joven matemático Lester S. Hill propuso en un artículo publicado en 1929 un conjunto de 4 ecuaciones con un sistema en el que se cifraría el texto en claro en bloques de 4 caracteres. Las ecuaciones eran las siguientes:

Y1 = 8X1 + 6X2 + 9X3 + 5X4 mod 26
Y2 = 6X1 + 9X2 + 5X3 + 10X4 mod 26
Y3 = 5X1 + 8X2 + 4X3 + 9X4 mod 26
Y4 = 10X1 + 6X2 + 11X3 + 4X4 mod 26

De las cuales X1, X2, X3 y X4 corresponden a los caracteres del texto en claro de cada uno de los bloques de 4.

Las ecuaciones anteriores provienen de la multiplicación de este bloque de 4 por una matriz K formada por una clave secreta, que siempre deberá ser N x N caracteres, siendo N el número de elementos de cada bloque, así por ejemplo, para el caso anterior que cifraremos en bloques de 4, la clave deberá poseer 16 caracteres, que se pueden completar con otros caracteres en el caso que no llegase a 16.

Las ecuaciones anteriores, por tanto provienen de lo siguiente:

Y1		8	6	9	5		X1
Y2	=	6	9	5	10	x	X2
Y3		5	8	4	9		X3
Y4		10	6	11	4		X4

Características de la matriz K

En primer lugar, cómo se ha comentado anteriormente, la matriz debe ser cuadrada en función al número de elementos a cifrar, en el ejemplo anterior se cifrarían bloques de 4, pero igualmente se pueden hacer con bloques de 3 o 5, en cuyos casos la clave debe ser de 9 y 25 respectivamente, ni uno más ni uno menos.

Si se trabaja con un alfabeto en módulo 26, alfabeto inglés, la clave no podrá poseer números que sobrepasen ese módulo, pues caería en la alguna equivalencia de dicho módulo, para eso se le asigna a cada letra un número, en este caso A=0-Z=26.

Para que el proceso pueda ser reversible, la matriz K ha de tener inversa, es decir, su determinante debe ser cero y el modulo N de dicho determinante debe ser distinto de cero, es decir, un determinante igual a 26 sería igualmente nulo, ya que el módulo es 0 , de lo contrario el mensaje no se podría descifrar y el sistema no valdría para nada. Este punto es el más importante, ya que es ahí donde radica su punto débil, ya que esta condición limita mucho el número de posibilidades a la hora de realizar un ataque por fuerza bruta.

Aspectos básicos de aritmética matricial

Para poder crear una clave válida para este sistema se deben poseer unos conocimientos básicos sobre las matrices que supongo muchos de vosotros tendrán, de igual modo pasaré a explicarlos para recordárselo a aquellos un poco mas perdidos.

Para que el proceso pueda tener un sentido inverso, y descifrarse, la matriz debe poseer una matriz inversa. La obtención de dicha matriz inversa se realiza mediante la siguiente ecuación:

K-1 = (TAdj(K)) / |K|

Donde K-1 es la matriz inversa de K, TAdj(K) es la transpuesta de la matriz adjunta de K, y |K| es el módulo de K.

La obtención de una matriz adjunta se debe eliminar la fija i y la columna j, y con los elementos restantes calcular el determinante. Veamos un ejemplo:

0	1	2
5	4	3
6	7	8

Para calcular el elemento 1,1 de la matriz adjunta de la anterior matriz, se elimina la fila 1, y columna 1, con lo cual nos quedan los elementos 4, 3, 7 y 8.

Para calcular el determinante de estos elementos, se multiplican los elementos de la diagonal principal menos el producto de los elementos de la diagonal secundaria. Hay que aclaran que la diagonal principal es de izquierda a derecha, y la segundaria de forma inversa, por lo tanto seria: (4x8)-(7*3)=11.

Esta misma operación se realizaría para obtener los 9 elementos de la matriz adjunta, lo cual



nos daría la siguiente matriz:

11	22	10
5	-6	-6
-5	-10	-5

La transpuesta es tan solo cambiar filas por columnas, es decir:

11	5	-5
22	-6	-10
10	-6	-5

Proceso de cifrado/ descifrado

Siguiendo con el ejemplo anterior, para la clave CIFRAHILL el mensaje M = CRIPTOGRAFIA CLASICA quedaría del siguiente modo:

$$\begin{pmatrix} Y1 \\ Y2 \\ Y3 \end{pmatrix} = \begin{pmatrix} C & I & F \\ R & A & H \\ I & L & L \end{pmatrix} \times \begin{pmatrix} C \\ R \\ I \end{pmatrix}$$

Esto nos daría el bloque: EIG

((2 x 2) + (8 x 2) + (5x2)) mod 26 = 4 = E
((18 x 18) + (0 x 18) + (7x18)) mod 26 = 8 = I
((8 x 8) + (11 x 8) + (11x8)) mod 26 = 6 = G

LA OBTENCIÓN DE UNA MATRIZ ADJUNTA SE DEBE ELIMINAR LA FIJA I Y LA COLUMNA J, Y CON LOS ELEMENTOS RESTANTES CALCULAR EL DETERMINANTE

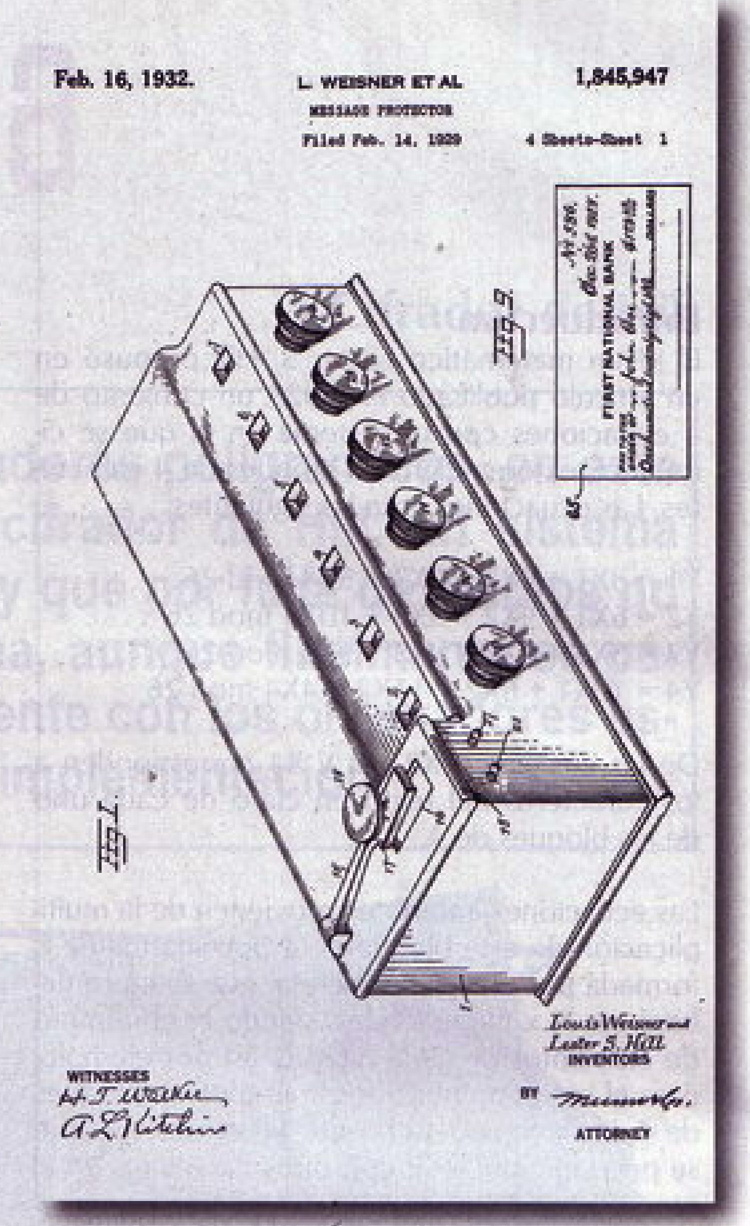
El criptograma resultaría de aplicar esta misma operación en cada uno de los bloques, recordando que el mensaje en claro debe completarse siendo el total de caracteres múltiplo del número de caracteres del bloque que deseemos cifrar.

El proceso inverso sería exactamente igual, salvo que se utilizaría la matriz inversa para el proceso de descifrado.

Seguridad

Este sistema presenta una desventaja a favor de un ataque por fuerza bruta. Si recuerdan, la matriz para poder poseer inversa deberá tener un determinante distinto de cero y que además el módulo N de dicho determinante fuese distinto de cero, esto quiere decir que no tuviese factor común con N, siendo N el número de elementos del alfabeto utilizado.

Por lo tanto, conociendo estos datos es fácil saber que no todas las matrices son válidas y por

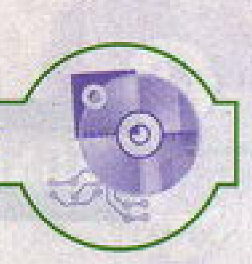


lo tanto, se descartarían para realizar un ataque, reduciendo considerablemente el número de combinaciones posibles. El número total de matrices en un alfabeto de módulo 27 y una matriz K de 4x4 tendremos 531.441 de las cuales solo son válidas 314.928, ya que una gran mayoría posee factor común con N. Esto puede resolverse utilizando un número primo, en cuyo caso solo se descartarían las matrices cuyo determinante sea igual a 0, pero no aquellas que posean factor común con N. Por ejemplo podría utilizarse el módulo 37, correspondiente a las letras del alfabeto y los números del 0 al 9.

Es claro comprender, que un ataque por estadística del lenguaje resultaría inútil, ya que el sistema rompe totalmente con dicha estadística, y cada carácter del criptograma depende de la posición global en la que se encuentre dentro del mensaje en claro, además depende igualmente del número de elementos de cada grupo, y es precisamente este su punto más fuerte, ya que aumentando el número de elementos se consigue aumentar la distancia de unidad, dependiendo cada vez de mas caracteres del mensaje original lo cual lo convierte en un sistema bastante robusto para la época.

TheBlooD


redes zombi
Preparan el ataque definitivo



Si no tomamos las medidas oportunas al conectarnos a Internet, nos exponemos a diversas amenazas entre las que se encuentran los ataques que ansían tomar los mandos de nuestra máquina de forma remota y utilizarla para cometer fechorías sin nuestro conocimiento. Junto con otros PCs, conformarán las conocidas como redes Zombi, una de las grandes amenazas de la actualidad y una nueva forma de delito cibernético.

Desde que la Red es lo que es, han existido individuos dispuestos a sacarle el máximo provecho haciendo uso de métodos que cuando no rozan la ilegalidad, la sobrepasan de lleno. La ciberdelincuencia se ha convertido en todo un "arte" que se supera constantemente, dejándonos a nosotros, los usuarios, vulnerables a robos, suplantaciones y demás actividades ilícitas. Hace algunos años, las empresas eran el objetivo principal, pero en la actualidad se ha experimentado un cambio drástico que amenaza a los usuarios de a pie. Y es que los tiempos cambian.

Antes, los desarrolladores de virus podían crear el caos en la red sólo por el mero hecho de demostrar que eran capaces de ello; los famosos 15 minutos de fama. Hoy en día los ciberdelincuentes valoran más el pasar desapercibidos y ganar dinero, dejar los ataques a redes empresariales y enfocarse en los PC personales. La prueba de ello es que en el último semestre de 2006 el 93% de todos los ataques fueron dirigidos contra el usuario doméstico, según un informe de Symantec. Los virus ya no son el enemigo, por lo menos no el más peligroso. Ahora, la amenaza es silenciosa, subrepticia, traicionera, y puede vagar por nuestro sistema sigilosa, esperando el momento de actuar para convertirnos en incautos cómplices de acciones ilegales, haciendo que nuestro ordenador forme parte de lo que se conoce como una red zombi.

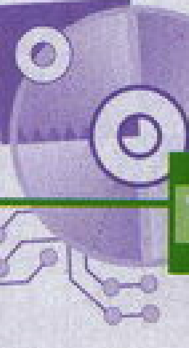
El amanecer de los muertos vivientes

Aunque quizás algo teatral, con el término Zombi se denomina a un ordenador que, tras ser infectado por algún tipo de malware, troyano, spyware o gusano específico, es usado por una tercera persona, de forma remota, para ejecutar actividades hostiles (gusanos famosos como Sobig, MyDoom o Bagle contienen este tipo de código malicioso). Un programa Zombi, o "Bot", es aquella aplicación que se controla a distancia y que convierte al PC objeto del ataque en un instrumento para propósitos deshonestos (a veces se hace extensiva esta denominación al propio PC infectado). Cuando se instala, proporciona al intruso un control absoluto del equipo, que ahora se encuentra en estado Zombi. A su vez, los ordenadores atacados forman redes Zombi, también llamadas Botnets o redes robot, y a los administradores de estas redes se les denomina botmasters.

Al principio, las víctimas propiciatorias eran equipos sin protección de antivirus y anti-spyware aunque esto ha evolucionado de tal manera que ahora afecta también a sistemas protegidos pero que no cuentan con las definiciones recientes de virus, gusanos y códigos maliciosos. Las redes Zombi se utilizan como plataforma para enviar correo no solicitado Spam coordinando un envío en el que una máquina sucede a otra en los intentos de entrega con pocos segundos de diferencia. En el momento en el que un equipo es infectado con un programa Zombi podrá ser utilizado por intrusos para generar ataques, para descargar programas pirata, incluir material pornográfico, o aplicaciones de intercambio a través de redes P2P, principalmente intercambio de archivos con formato mp3 y mpeg. También podrá dirigir ataques sincronizados de denegación de servicio (DoS) distribuido a través de la red, provocando saturaciones y lentitud en las redes. Así, grupos organizados pueden controlar miles de sistemas infectados creando redes capaces de generar grandes cantidades en tráfico procedentes de multitud de fuentes en Internet para atacar una sola red o servidor, a menos que la víctima ceda a un chantaje económico (el riesgo para el delincuente es mínimo porque se escuda detrás de estos equipos). Un arma muy peligrosa que puede ser usada para liderar conductas delictivas a través de Internet, y que está detrás de los envíos de Spam (el 80% de correo basura se envía a través suyo), Phishing o DoS, aunque una de las mayores preocupaciones viene derivada de que pueden ser usadas para lanzar ataques DoS distribuido como ya ocurriera en el 2000. Un colapso de 100.000 peticiones provenientes de diferentes lugares al mismo tiempo.



Un PC Zombie es controlado remotamente con propósitos malintencionados

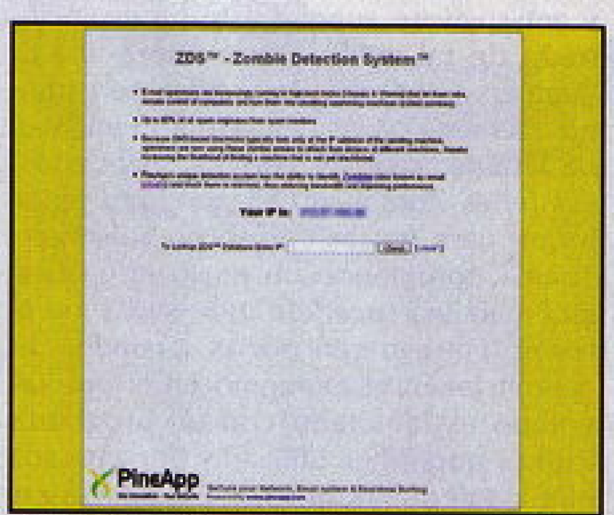




Mapa de Puntos calientes de donde viene el Spam

Una buena red Zombi debe constar de unos 10.000 PCs infectados. Este número ofrece además cierto reconocimiento para el hacker que lo logre, brindándole un punto de apoyo importante de cara a vender las redes Zombi a spammers y a quienes organizan ataques contra sitios web. De momento, parece que el negocio va "viento en popa" porque, según distintos estudios, entre el 40 y el 80 por ciento de todo el correo basura se envía actualmente a través de PCs domésticos infectados sin que el usuario sea consciente de ello. Por si fuera poco, el propietario del ordenador Zombi aparece como el autor del spam ya que se utiliza su nombre y email en los ataques, convirtiéndolo así en cómplice inesperado al aparecer el nombre del usuario detrás de actividades ilícitas. Los datos son reveladores: en diciembre de 2005 el Spam era responsable del 94% del tráfico de correo electrónico y en 2006 el crecimiento era del 147%. Vint Cerf, uno de los creadores de Internet y actualmente "Evangelista" de Google, ha sugerido que casi 40 millones de ordenadores conectados a la Red, en todo el mundo, podrían estar infectados con troyanos. Según los expertos, un 11% de los ordenadores con acceso a Internet forman parte de Botnets, lo que representa millones de Zombies, con un ritmo de infección de 250.000 ordenadores diarios, beneficiadas por el aumento de usuarios en la Red y las mejores velocidades de conexión y ancho de banda. Se calcula que hay cerca de 50.000 ordenadores enviando Spam y contenido maligno en cualquier momento, PCs que "trabajan" durante 45 minutos, transcurridos los cuales dejan de trabajar, dificultando labores de identificación. Según la compañía de seguridad Prolexic, China es el país más afectado del mundo y Asia tiene la mitad de todos los sistemas infectados del planeta, lo que unido a las mejoras constantes de los ciberdelincuentes puede suponer que nos encontramos ante un nuevo hito en los niveles de spam y virus en correos electrónicos.

UNA BUENA RED ZOMBI DEBE CONSTAR DE UNOS 10.000 PCS INFECTADOS. ESTE NÚMERO OFRECE ADEMÁS CIERTO RECONOCIMIENTO PARA EL HACKER QUE LO LOGRE



La herramienta ZDS permite verificar gratuitamente si eres un Zombie

La efectividad de las Botnets ha generado un mercado negro virtual en el que se ofertan sus servicios. El precio depende de su tamaño: cuantos más PCs la compongan, mayor efectividad en el ataque, pudiendo comprarse un troyano para crear una red ilegal de robots por unos 4.000 euros. Pero es difícil determinar los costos de una Botnet al no conocerse la estimación real de equipos contagiados por países o de los millones de PCs que se encuentran conectados a Internet. Se cree que el costo de un equipo Zombi en ambientes underground ronda los 10 centavos de dólar por acceso compartido en una máquina comprometida. En la no compartida, es decir, para un acceso exclusivo al equipo, se vende en 25 centavos de dólar y se ofrecen descuentos en grandes cantidades.

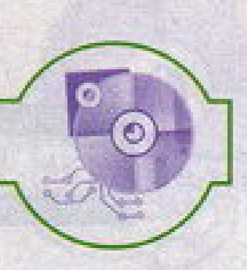
Los pagos pueden realizarse por Paypal, en efectivo, o a través del correo a un buzón en cualquier parte. El acceso a los equipos se realiza una vez efectuado el pago y confirmado. El trueque también es moneda habitual y es la base de los negocios underground. Aquí se intercambian números de cuentas bancarias, de tarjetas de crédito (las mafias dan seis euros por los datos de una tarjeta) o bases de datos de emails, entre otros. Por ejemplo, se intercambian 30 mil equipos Zombi por 20 números de tarjetas de crédito.

Crónica de una infección

En un principio los programas bot se usaron para acceder a equipos remotos, instalar servidores, y establecer recursos y anchos de banda gratuitos en equipos de terceros (los inicios de la computación distribuida). Se desarrollaron programas automáticos que permitían a los operadores de los servidores la instalación automática en diversos equipos alrededor del mundo, con un mínimo de esfuerzo.

A inicio de los 90 los bots eran usados en los IRC (Internet Relay Chat, un sistema de conversación en tiempo real para usuarios de Internet) para mantener el canal activo cuando se daban desconexiones durante una sesión, o para compartir archivos entre usuarios. El auge de los servidores IRC hizo que aumentara el número de usuarios que chateaban, lo que obligó a los operadores a desarrollar una forma de controlar y administrar estas conversaciones. Esto supuso el inicio de los "baneos", o expulsión de usuarios de este tipo de foros si se sobrepasaban. Esta situación supuso el caldo de cultivo para que usuarios rechazados desarrollaran técnicas y métodos para dañar a los servidores y, en consecuencia, los canales correspondientes. Por primera vez pudo verse la implementación de ataques del tipo DoS y, posteriormente, ataques del tipo DoS distribuido, mucho antes de que fueran utilizados para atacar a las empresas (de hecho los bots actuales cumplen con el RFC 1459, el documento donde se define el estándar del servicio IRC, que les permite contar con un canal de comando y control a través del canal IRC).

El uso de servidores IRC para "chatear" se expandió, así como su control de manera remota. Se introdujeron nuevas formas de utilización, a la par de servidores para en-



viar correo no solicitado. Con ello, los intrusos se dieron cuenta que podían controlar no sólo estos servidores, sino que podían hacerlo de forma remota y que ello bastaba con emplear programas Zombi. Las corporaciones dieron el siguiente paso implementando medidas para eliminarlos, bloquearlos y protegerse así que nacieron los virus, gusanos, troyanos, spyware y toda clase de códigos maliciosos como forma de sortear esta barrera, usando ingeniería social para infectar y crear redes dependientes de programas Zombi.

Microsoft, realizaba en 2005 un curioso experimento. Durante tres semanas conectó a Internet una máquina desprotegida, como señuelo. Diversos spammers intentaron conectarse a la máquina más de 5 millones de veces e intentaron enviar alrededor de 18 millones de mensajes de correo electrónico. El frenesí de los spammers fue tal que Microsoft presentó querellas contra 13 de ellos. En noviembre de ese año, según Sophos, si un equipo sin protección antivirus o sin cortafuegos se conectaba a Internet, existía un 50% de probabilidades de "Zombificarse" en 12 minutos, y durante los seis primeros meses de 2006 Symantec contabilizó más de 4,5 millones de ordenadores Zombi. A finales de 2006 se sufrieron una serie de ataques sin precedentes a gran escala de manos del gusano de correo Warezov, creado y diseminado con el objetivo de utilizar los equipos infectados como servidores proxy de correo en el futuro. Las primeras muestras del ataque hicieron su aparición en Internet en octubre de 2006. Hasta 20 variantes aparecieron en 24 horas, creando una red Zombi gigante.

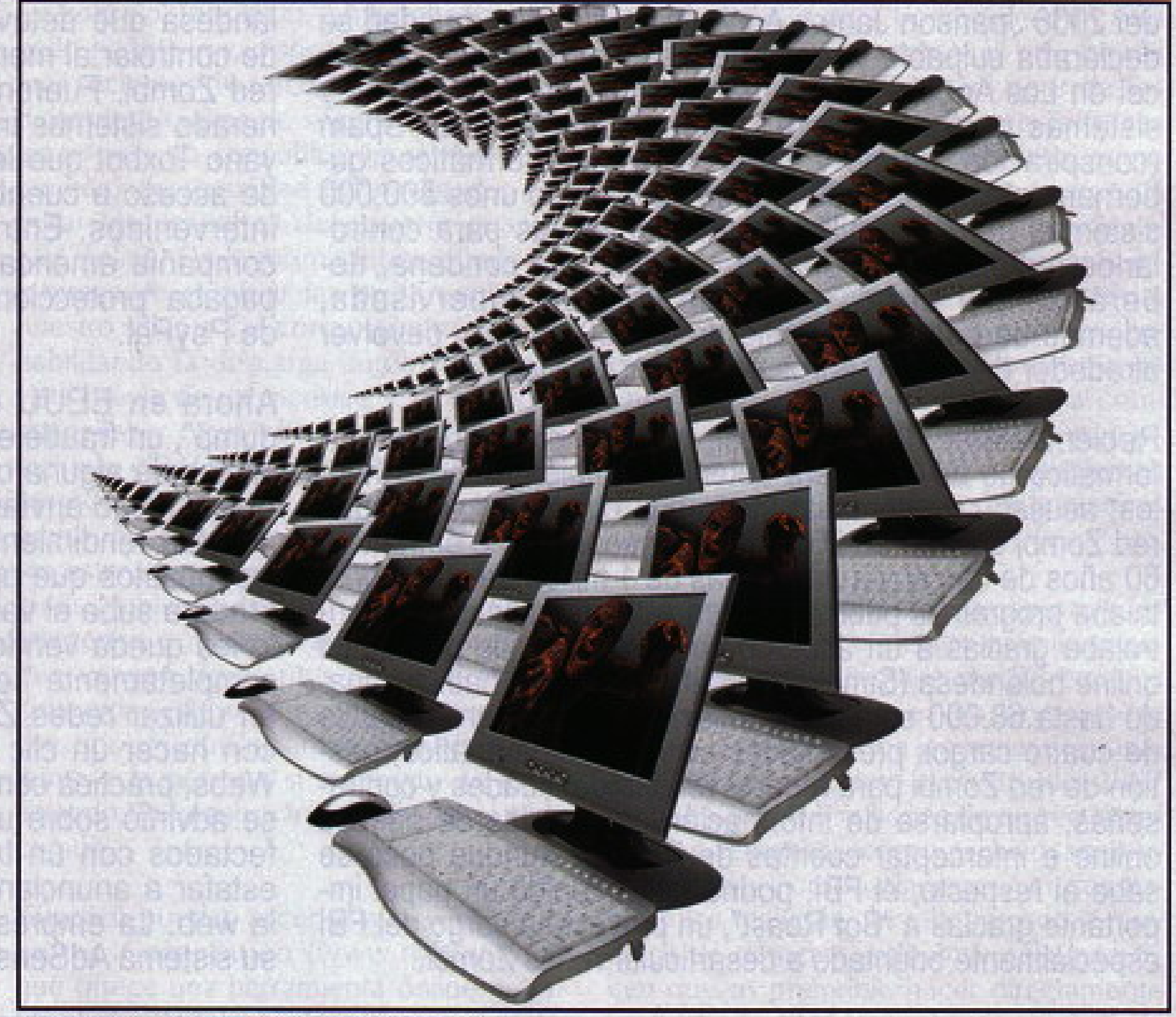
LA EFECTIVIDAD DE LAS BOTNETS HA GENERADO UN MERCADO NEGRO VIRTUAL EN EL QUE SE OFERTAN SUS SERVICIOS. EL PRECIO DEPENDE DE SU TAMAÑO

Ya en enero de 2007 surgió otra oleada de correos electrónicos con un troyano, que descargaba otros componentes (rootkit) al ordenador víctima. Fue bautizado como "Storm Worm" (Gusano tormenta), aunque oficialmente recibió el nombre de Zhelatin. Al igual que Warezov, Zhelatin convierte el PC cautivo en un servidor Proxy troyano que podía ser utilizado como una plataforma de envíos masivos de correo electrónico y para lanzar ataques de DoS. Curiosamente el blanco del ataque fueron los sitios utilizados por los autores de Warezov junto a varios otros sitios que pertenecían a organizaciones antispam. Había estallado la guerra entre los grupos detrás de ambos gusanos y, quizás, uno de los problemas más graves de Internet en los últimos años. La lucha de dos titanes con nosotros en el centro.

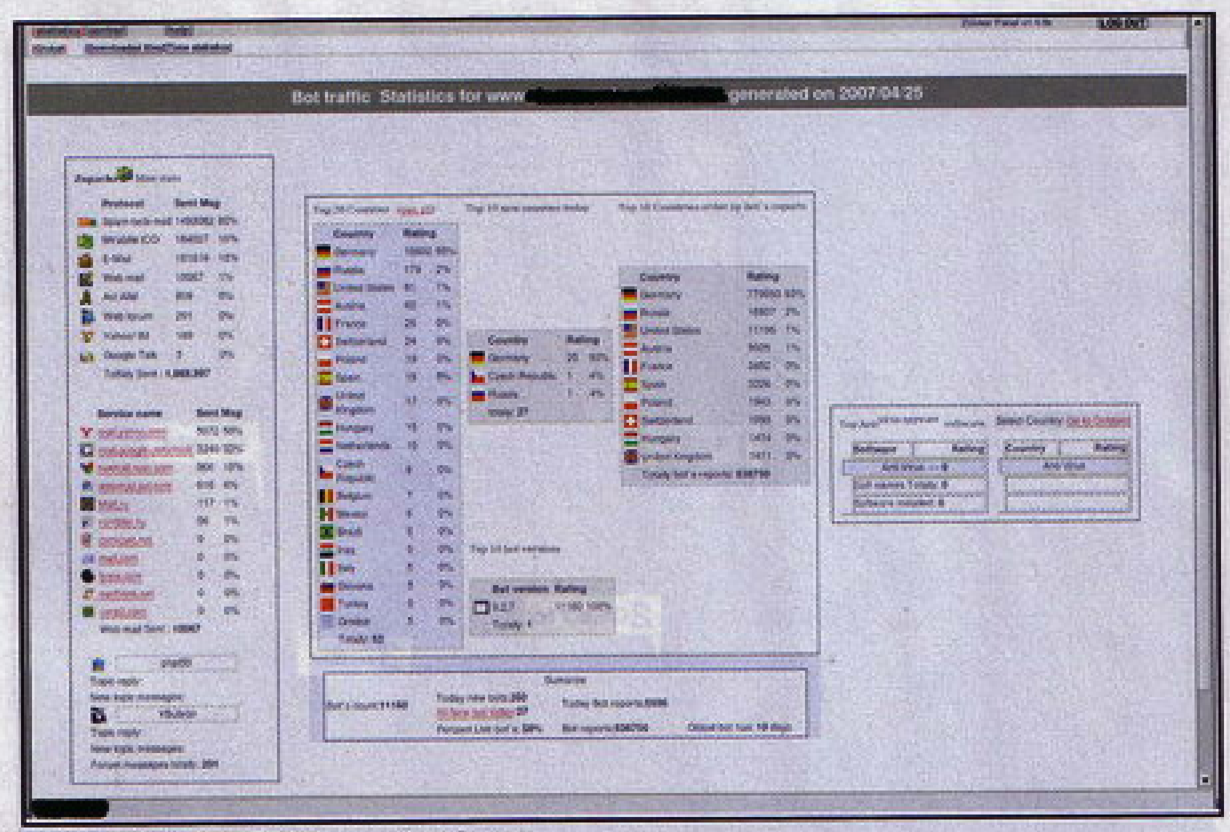


Representación visual de un ataque

En mayo de 2007, PandaLabs descubría ZUnker, un programa creado por ciberdelincuentes para gestionar ordenadores Zombies que formaran parte de sus Botnets que se extendían por 54 países. Esta aplicación contaba con un apartado de estadísticas, gráficas para ver la efectividad de cada bot, el número disponible y su actividad organizada por día y mes. Organizaba bots por países y permitía saber en



Un ejercito de PCs zombies está listo para atacar



Aspecto de programa Zunker que controla Botnets

los bots que descargaran otros archivos en las máquinas infectadas, por ejemplo, malware (troyanos, adware, virus).

Hoy en día algunos ataques hasta han sido bautizados: el Ping de la muerte (los bots crean paquetes de datos de gran tamaño y los envían a la víctima), el Mail-bomb (se envía una cantidad masiva de emails tirando abajo los servidores de correo), el Ataque Smurf (se envían mensajes con paquetes ICMP a los reflectores que los reenvían a la victima) o el Teardrop (los bots envían partes de un paquete ilegítimo y el sistema de la víctima intenta recomponer las partes en un solo paquete y como resultado el sistema cae).

El ataque y el arte de la prevención

La creación de una red Zombi conlleva varias etapas. En la primera se determina el vector de infección (correo, vulnerabilidad del sistema operativo o de alguna aplicación, etc.) y, a continuación, los métodos de ataque que usarán los bots. Una vez hecho esto, se obtiene o desarrolla el software malicioso y se procede a vulnerar un servidor de IRC e instalar el bot en

todo momento cuántos había en cada lugar, cuánto spam habían enviado o con qué programa (gmail, IM, foros..,), etc. También permitía controlar la red de bots ordenándoles las acciones a llevar a cabo (por ejemplo enviar spam) y diseñar el contenido con plantillas en función del tipo de destinatario del mensaje. Incluso era capaz de informar del número de bots que permanecían activos para ordenar a

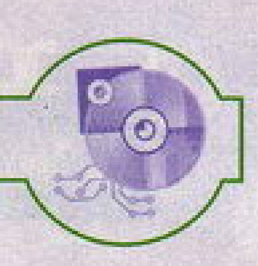
>>> Ladrones de guante... virtual

Con cada vez más frecuencia oímos hablar de casos que tienen a las redes Zombi como protagonistas. En mayo del 2006 Jeanson James Ancheta de 20 años de edad se declaraba culpable y era condenado a 57 meses de cárcel en Los Angeles, California, por utilizar ordenadores y sistemas para dañar redes informáticas y enviar Spam (conspiración, fraude y dañar sistemas informáticos gubernamentales). En 2004 había intervenido unos 500.000 sistemas (algunos militares) mediante bots para controlarlos remotamente. Una vez cumplida la condena, deberá cumplir otros 3 años de libertad supervisada, además de pagar una multa de 11.800 euros y devolver alrededor de 40.000 euros de ganancias ilícitas.

Recientemente John Schiefer, experto en seguridad informático de 26 años, era detenido también en Los Angeles, acusado de controlar, junto con otros cómplices, una red Zombi de más de 250.000 ordenadores y se enfrenta a 60 años de cárcel y a pagar más de 1 millón de euros. Instalaba programas publicitarios en estas máquinas que controlaba gracias a un acuerdo con una firma de publicidad online holandesa (Simple Internet) con la cual habría ganado hasta 68.000 euros en comisiones. Se declaró culpable de cuatro cargos presentados por fraude informático, gestión de red Zombi para robar y vender identidades y contraseñas, apropiarse de información de cuentas de bancos online e interceptar cuentas de PayPal. Aunque poco se sabe al respecto, el FBI, podría haber tenido un papel importante gracias a "Bot Roast", un proyecto a cargo del FBI especialmente orientado a desarticular redes Zombi.

Pero en Europa también hemos tenido nuestra dosis de acción policial, en este caso de manos de la unidad holandesa que detuvo a tres jóvenes en Breda acusados de controlar al menos 10.000 ordenadores mediante una red Zombi. Fueron detenidos bajo cargos de haber vulnerado sistemas informáticos e instalado en ellos el troyano Toxbot que les enviaba contraseñas e información de acceso a cuentas e inicio de sesiones desde los PC intervenidos. Entre otras lindezas amenazaron a una compañía americana con realizar un ataque DoS si no pagaba "protección" y habría robado cuentas de usuarios de PayPal.

Ahora en EEUU está en auge el llamado "pum and dump", un fraude en el que los delincuentes compran acciones de alguna compañía cuando están a la baja en la Bolsa, luego envían spam con falsas estimaciones sobre un gran rendimiento en el futuro, vendiendo acciones a los incautos que piquen, y haciendo que la oleada compradora suba el valor de la acción. A los delincuentes sólo les queda vender las suyas y hacer un buen negocio completamente "legal". Pero la última hazaña consiste en utilizar redes Zombi para ganar dinero simplemente con hacer un clic en los banners de publicidad de las Webs, práctica conocida como clickfraud. Recientemente se advirtió sobre una red zombi de 115 ordenadores infectados con un troyano especialmente diseñado para estafar a anunciantes haciendo clic en sus anuncios en la web. La empresa más perjudicada sería Google, con su sistema AdSense.

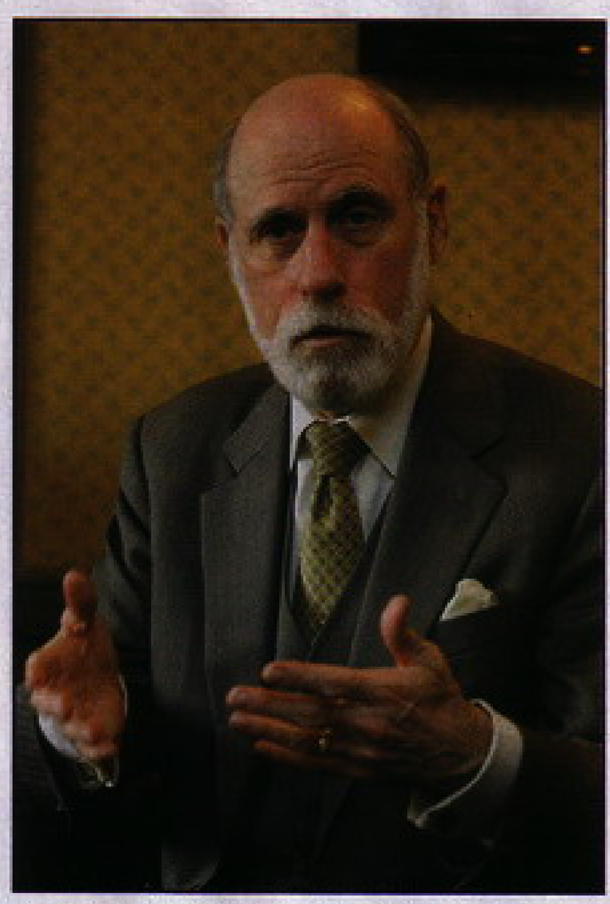


las máquinas de los usuarios víctimas. La inversión es mínima, teniendo en cuenta el abanico de delitos que pueden cometerse gracias al ancho de banda gratuito que resulta de controlar miles de ordenadores, muy superior al de una gran compañía. Pueden enviarse instantáneamente millones de mensajes fraudulentos, Spam, virus que roban datos bancarios y hasta chantajear empresas, amenazándolas con lanzar redes Zombi contra ellas.

La cronología de un ataque comienza al recibir un email o navegar por una web sospechosa (por ejemplo con fotos sugerentes de famosos). Al hacer clic sobre cualquiera de los elementos se corre el riesgo de descargar silenciosamente un programa que se instale en nuestro ordenador y que la prepare para ser utilizada de forma remota sin nuestro consentimiento. Si los afectados son empresas, en ocasiones apenas trasciende y las investigaciones son secretas, por miedo a minar la confianza de los clientes.

Detectar que hemos sido infectados por un bot es más complicado que localizar otras infecciones ya que, al tratar de pasar desapercibido, es probable que nuestro PC no presente ningún comportamiento extraño o que éste sea muy leve. No obstante, y sin caer en la paranoia, existen algunos síntomas asociados de contagio. Por ejemplo que la conexión a Internet sea más lenta de lo habitual, que el disco duro trabaje (hace ruido) aunque no le solicitamos tareas, que el teclado o el ratón funcionen erráticamente o que obtengamos respuestas a correos electrónicos que no hayamos enviado. En un PC Zombi, además de los puertos de comunicaciones utilizados por las aplicaciones habituales, hay puertos abiertos al servicio del atacante. Para localizarlos y saber qué están haciendo, puedes ejecutar el comando "netstat" en la consola MS-DOS (en Windows XP a través de Inicio > Ejecutar, y escribiendo "cmd") y analizar los resultados.

Defenderse es una tarea que debe hacerse en dos frentes. El primero de ellos es del lado de los servidores IRC que deben contar con las medidas de seguridad de cualquier servidor. Sin embargo, el elemento más frágil en la ecuación es el propio usuario que debe contar con todos los elementos de seguridad implementados (firewall personal y antivirus). También es recomendable instalar medidas adicionales de seguridad para eliminar programas Spyware (soluciones como Adware o Spybot Search & Destroy son excelentes elecciones) y monitorizar el flujo de datos en la red interna y no solamente en los perímetros.



Vint Cerf, uno de los creadores de Internet, advierte de que las redes Zombies son ya una pandemia

LA CRONOLOGÍA DE UN ATAQUE COMIENZA AL RECIBIR UN EMAIL O NAVEGAR POR UNA WEB SOSPECHOSA (POR EJEMPLO CON FOTOS SUGERENTES DE FAMOSOS)

En cualquier caso, la vigilancia será el mejor consejo. Esto incluye mantener actualizado el antivirus, disponer de los parches más recientes de Microsoft, realizar periódicamente copias de seguridad, evitar páginas web no confiables, incrementar las medidas de seguridad del navegador y limitar los derechos del usuario cuando esté online. De la misma forma puede ser interesante cambiar las preferencias de nuestro cliente de correo electrónico inhabilitando la descarga automática en la vista previa de un mensaje, y bloqueando imágenes y otros contenidos de Internet, incluido el HTML, de ser descargados automáticamente en tu PC. Y claro, ni se te ocurra hacer clic en enlaces de mensajes sin estar seguro de adónde te llevan, ni abras archivos adjuntos que parezcan ser imágenes o algún otro tipo de archivos que vengan de fuentes desconocidas, o conocidas, si no esperas un adjunto de ese tipo. Si dudas, antes de abrirlo pregunta a la persona si realmente te lo ha enviado. Pero sobre todo utiliza el sentido común.

También puedes acceder a la web de PineApp Corporation (www.rbltest.com) que ofrece una herramienta online gratuita, el Zombie Detection System (ZDS), que analiza al instante si tu PC o la red de una empresa están infectados y pertenecen a alguna red Zombi conocida. Teclea allí tu IP y compruébalo.

En el caso de que tu ordenador ya esté infectado y se haya convertido en un Zombi, aún puedes salvarlo pero deberás buscar un buen programa de eliminación de virus para romper la conexión entre el PC y el hacker. Si esto no funciona, en ocasiones la única opción que queda es formatear el disco duro y volver a empezar. De ahí la importancia de hacer regularmente backup de tus datos. Y antes recuerda pasar a tus copias de seguridad un antivirus para asegurarte de que no están infectados.

Si formas parte de una entidad que está sufriendo el ataque, como administrador del sistema hay algunas cosas que podrás hacer para prevenir una catástrofe. Puede limitar la cantidad de tráfico permitida en el servidor, aunque ten en cuenta que esto conllevará restringir también las conexiones legítimas a Internet. Si se puede determinar los orígenes de los ataques será posible filtrar el tráfico pero por desgracia los ordenadores pueden "disfrazar" sus direcciones con técnicas de spoofing, inhabilitando estos filtros.

El Superordenador más potente del mundo se llama "Storm"

Si todos los ordenadores son activados simultáneamente para bombardear un sitio web o servidor, el acceso al sitio queda totalmente bloqueado. En el peor de los casos, un ataque de tales características puede afectar a un país completo, como ocurriera en Estonia el pasado verano. El ataque ya se ha convertido en caso de estudio y, para muchos, es el primer acto real de guerra cibernética de la historia. Según los expertos, el ataque fue excepcional en el sentido que no provenía de una fuente específica, sino de una compleja red de sistemas coordinados, que incluían desde scripts primitivos distribuidos en ordenadores personales, hasta ataques coordinados en redes Zombi.

Visto esto, es lógico que las autoridades estén alertas ante el peligro más inminente: la red Zombi formada por los equipos contaminados con el gusano Storm Worm. Este tuvo una enorme propagación durante el último semestre del 2007 (con más de 415 millones de correo spam en dos semanas), como archivo adjunto de emails y como enlaces engañosos hacia sitios malignos. Instala un rootkit muy difícil de detectar y eliminar - algunos dicen que es preferible hacer directamente un backup y formatear el sistema - que es-

cucha Internet a la espera de un comando que lo haga entrar en acción. Al más puro estilo "Candidato de Manchuria".

Sin embargo, lo curioso de Storm es que el comando de activación no ha sido enviado aún. Según Future Zone, actualmente habría 1,7 millones de PCs infectados con este gusano en todo el planeta, esperando el comando que les active como Zombies. De momento una pequeña parte del ejército durmiente se usa para propagar el gusano, en tanto que otra, igual de reducida, realiza ataques de prueba contra sitios antispam, a modos de ensayos previos a un inminente gran ataque. Según MessageLabs y a través de la comunidad antispam (y la web SpamNation) se han reportado en los últimos meses escaramuzas de DoS de manos del grupo Zhelatin que se tiene como sospechoso del crecimiento del gusano Storm. Según SpamNation, los operadores de esta red venden sus servicios a quienes deseen realizar ataques y se estima que están en condiciones de generar varios cientos de gigabits por segundo de tráfico digital destructivo hacia los sitios que deseen atacar y tienen los recursos para aislar países completos de Internet. Por ahora se desconoce quién controla la gigantesca red de Zombies, ni cual es su objetivo.

Con casi 2 millones de máquinas infectadas a nivel mundial, entregándole acceso a enormes capacidades de procesamiento y entre 1 y 10 Petabytes de RAM (un PB equivale a mil millones de megabytes) la convierte en el mayor superordenador del mundo. Si fuera activado para un ataque simultáneo llevaría a cabo el mayor acto de sabotaje cibernético visto hasta el momento. Se estima que la capacidad de procesamiento de esta red de Zombies es



El FBI ya se lo toma en serio y ha creado un proyecto para perseguir redes Zombi

ES LÓGICO QUE LAS AUTORIDADES ESTÉN ALERTAS ANTE EL PELIGRO MÁS INMINENTE: LA RED ZOMBI FORMADA POR LOS EQUIPOS CONTAMINADOS CON EL GUSANO STORM WORM

superior a los 10 superordenadores más potentes de la actualidad trabajando simultáneamente, según el catedrático de informática Peter Gutmann, de la Universidad de Auckland, Nueva Zelandia. Y lo hace mediante la cuenta de la vieja: mientras que la red Storm cuenta con un máximo de 10 millones de procesadores, el superordenador de IBM, Blue Gene/L, que preside la lista Top 500, "sólo" tiene 128.000 procesadores. Además, la superioridad de memoria de Petabytes de Storm es prodigiosa (considerando que cada uno de los PC tiene alrededor de 1 GB en RAM, contra 32 los terabytes para la mayor supercomputadora del mundo).

La seguridad 2.0

Neutralizar una red Zombi es una tarea compleja ya que no existe un punto central de comando visible. Se requiere gran coordinación entre equipos y expertos de seguridad, eso sin contar con leyes actualizadas. Por si fuera poco el fenómeno crece y las nuevas amenazas son más sofisticadas e ingeniosas: Troyanos desechables, acceso a bases de datos privadas, redes Zombi y virus para móviles serán las principales amenazas para 2008. Por si fuera poco, los antivirus tradicionales ya no son suficientes. Ahora tiene que integrar armas contra gusanos, troyanos y Phising, y que para proteger la información, incluyan soluciones para realizar backups casi en tiempo real. Herramienta de seguridad 2.0 para la Web 2.0.

En los foros del poder ya se habla de ello. Existe una posibilidad entre cuatro de que tu ordenador forme parte de un ejército silencioso. Una red de máquinas esclavizadas que se venden al por mayor a quienes quieren derribar una web por saturación o enviar Spam. Vinton Cerf señalaba en Davos que la extensión de estas redes Zombies había alcanzado ya dimensiones de pandemia, con 150 millones de ordenadores (el 25% de los conectados a Internet) controlados por personas ajenas a su propietario. No parece que el funcionamiento de la Red esté aún amenazado pero redes Zombi como Store podrían contradecir esto, ¿hasta cuándo?

Nicolás Velásquez Espinel<

>>> España en el punto de mira

Varios son los países que tienen el dudoso honor de pertenecer a plataformas Zombies responsables de los envíos de Spam. España se encuentra en el quinto puesto y puede que en breve luche por las medallas, detrás de Francia y el triunvirato formado por Estados Unidos, China y Corea del Sur, que ya llevan meses reduciendo sus niveles de emisión. España ha pasado en dos años de generar el 1% del spam mundial al 6%, y Madrid ya es la ciudad con el mayor número de Zombies del mundo, según Symantec.

De momento España se considera como un país de tránsito, no un emisor directo, lo que significa que ni siquiera somos los autores intelectuales si no meros instrumentos de delito... sobre todo para enviar mensajes de Phishing (hacerse pasar por una entidad bancaria para robar datos de acceso como número de cuenta y contraseña, que después los delincuentes usarán para robarle). La red Telefónica España (segundo proveedor del mundo en correos eléctricos enviados con un volumen de 330 millones diarios) es posiblemente la más empleada para el envío de este tipo de correos.

Según el observatorio Zombie Stats, de la empresa estadounidense Ciphertrust, en una semana se detectan casi 50.000 nuevos ordenadores zombi en España, y 150.000 en un mes, de los cuales la mayoría son "equipos residenciales" (o sea, de particulares), con conexiones de banda ancha y cuyos propietarios no tienen ni idea de que un criminal los controla remotamente.

LO MEJOR PARA TU MOVIL

MENSAJES AL 7477



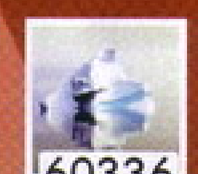
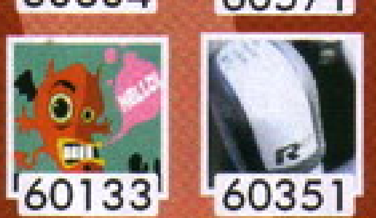
Envia ARIMAG + EL CODIGO
al 7477 Ej: ARIMAG 50406







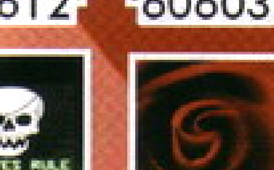


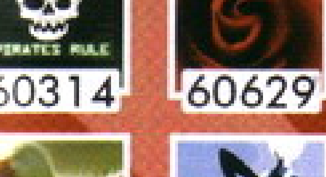





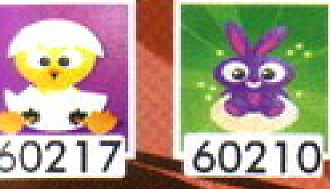














60162	60166	60163	60676	60169
60156	60135	60614	60673	60150
60326	60626	60604	60571	31585
60337	60336	60133	60351	40077
60613	1009	60349	60599	60660
60600	60350	60601	60609	60598
60612	60603	60620	60602	60617
60314	60629	60622	60619	60671
60625	60168	60161	60154	60171
60217	60210	60303	60289	60152
60649	60651	60656	60657	60674

Envia ARPOLI + EL CODIGO
al 7477 Ej: ARPOLI 50406

50406 Gorillaz - Dirty Harry
50393 Red Hot Chilli Peppers - Dani Ca
50375 Fito y Fitipaldis - Soldadito Marin
50374 Extremoduro - Golfa
50291 Freestylers feat. Petra - Told You
50264 Green Day - Wake Me Up When
50245 Moby - Dream About Me
50080 Simple Plan - Welcome My Life
50068 Green Day - Boulevard Of Broke
50063 Gorillaz - Feel good inc
50061 Weezer - Beverly Hills
50058 Good Charlotte - Just Wan Live
50312 The Chemical Brothers - Galva
50155 Fatboy Slim - Slash Dot Dash
50146 Neng - Soy persona
50145 Neng - Que pasa Neng
50134 Carlinhos Brown y Dj Dero
50046 Chemical Brothers - Believe
50388 El Koala - Opa yo viace un corra
50353 Mattafix - Big City Life
50352 La Cabra Mecanica - La uña de
50348 The Rolling Stones - Rain fall do
50346 Simple - Crazy
50343 Nickelback - Far Away
50342 Hoy no me puedo levantar - Un..
50341 Goldfrapp - Number one
50332 Pastora - Dia tonto
50330 Modestia Aparte - Cosas de la.
50329 Jamie Cullum - Mind trick
50321 Pain - Shut Your mouth V2
50318 El Barrio - Querida enemiga
50408 Jean Michel Jarre - Oxygene
50407 Hari Mata Hari - Lejla (Eurovision)
50405 Fabrizio Faniello - I do (Eurovision)
50404 Elena Risteska - Ninanaina (Euro..)
50403 Dima Bilan - Never Let You go (Eu)
50400 Andre - Without Your Love (Euro..)
50391 Gypsy Kings - Hotel California
50390 Gloria Gaynor - I will survive
50389 Carlos Jeans - Have a nice day
50381 King Africa - Paquito el chocola..
50380 Complices - LLámame
50379 Victor - The fool on the hill
50378 Zucchero y Mana - Baila morena
50377 Scorpions - Winds of change
50376 Juanes - Nada valgo sin tu amor
50372 Ennio Morricone - La muerte..
50370 Anastacia - Left outside alone
50369 Alberto Iglesias
50368 Sergio Rivero - Me Envenena
50366 Niña Pastori - Tu me camelas
50363 Edurne - Despierta
50360 Coti y Paulina Rubio - Otra vez
50359 Belanova - Me pregunto
50358 Tara Blaise - The Three degrees
50355 Richard Ashcroft - Break the night
50354 OT 2005 - Batlika Medley
50351 Kelly Clarkson - Behind these hazel
50350 Chambao - Sueño y muero
50349 Bono Feat. Mary J Blige - One
50345 Sidonie - Joe
50344 Pablo Moro - Vodka y caramelos

Envia ARREAL + EL CODIGO
al 7477 Ej: ARREAL 50406

50397 Nina Simone - (Spot Audi A4)
50395 Marvin Gaye - (Spot Movistar)
50347 Andy Williams - (Spot Honda)
50338 Dennis MCCarthy - BSO V
50227 tangagirls
50223 nike_brasil
50222 martini
50212 cocacola
50383 Amelie BSO - La Valse Damelie
50382 Amelie BSO - Jy suis jamais alle
50363 Henry Manciny - La pantera rosa
50276 Soundtrack - Rocky
50275 Soundtrack - Pretty Woman
50244 Soundtrack - Pink Panther
50243 Soundtrack - 007 James Bond
50209 topgun
50208 tiburon
50207 halloween
50206 thegoodthebadandtheugly
50205 starwars
50204 spidemanII
50203 silenciodeloscorderos
50202 shrek2
50398 Pignoise - Nada que Perder
50368 Soundtrack - Revelde Way
50367 Soundtrack - Perdidos
50366 Soundtrack - Mujeres desespe..
50365 Soundtrack - Dr. House
50237 uefachampionsleagueofficio
50236 xfiles
50235 thesimpsons
50234 sesamestreet
50233 aquinohayquienviva
50232 knightrider
50231 willandgrace
50230 twinpeaks
50229 cheers
50228 teletubbies
50226 southparkth
50225 sensacion_vivir
50224 pokemon
50221 macgyver
50220 garfield
50219 flinstones
50218 familia_addams
50217 falconcrest

Para WAP y compatibles con fondos a color. Precio del SMS 1,20 + I.V.A. Servicio de ocio y entretenimiento Revisa el manual de tu terminal para verificar compatibilidad. Recuerda que para descargar contenidos necesitas tener WAP habilitado.

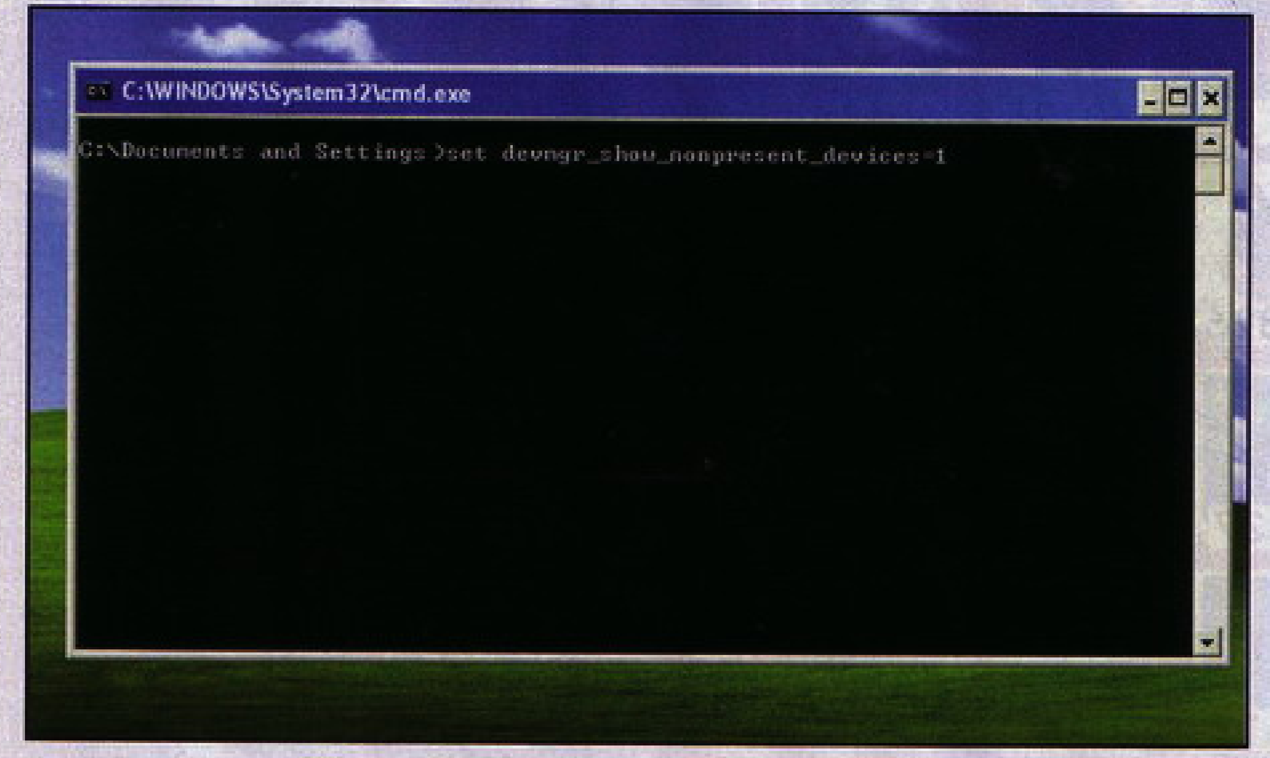
Identificar dispositivos USB que se hayan conectado alguna vez

Nuestro sistema podrá decirnos tantas cosas como las que se nos ocurra querer saber aunque será de vital importancia saber antes qué preguntar y de qué manera. Así descubriremos por ejemplo si se han conectado dispositivos USB sin nuestro conocimiento, lo que podría ser síntoma de vulnerabilidad de nuestra seguridad.

Los dispositivos USB han supuesto con toda seguridad una revolución en los últimos años, convirtiéndose en un sistema de almacenamiento y compartición de datos fiable y universal que ha relegado por ejemplo las disqueteras al oscuro abismo de los objetos sin uso gracias a las llaves USB. Pero además ha supuesto una vuelta de tuerca a la conectividad facilitando la interconexión dinámica de determinados sistemas como impresoras o discos duros externos, entre otros muchos. Recordamos que hace años para conectar y hacer funcionar estos elementos era necesario apagar, conectar, encender y configurar posteriormente estos elementos en un proceso que se hacía realmente tedioso.

La comodidad de conectar un dispositivo a nuestro PC y poder utilizarlo de forma inmediata ha agilizado enormemente la forma de trabajar pero también se ha convertido en un nuevo agujero potencial de seguridad en nuestros sistemas. Alguien podría conectarse a nuestra máquina enchufando un pendrive a la misma para sustraer información y lo cierto es que si no estamos presentes, poco podemos hacer para evitarlo. Sin embargo existe una forma en Windows XP que, aunque no evite el robo, si que puede darnos ciertos detalles que pueden revelarnos que se ha conectado algún tipo de dispositivo USB sin nuestro consentimiento.

Gracias a este método podremos identificar de un plumazo en el administrador de dispositivos del sistema los distintos periféricos que se hayan conectado a nuestra interfaz USB, de esta forma podremos saber qué dispositivos se han conectado y podremos ver si alguna vez se ha usado este puerto para conectar algo sin nuestro consentimiento.



Desde la línea de comandos establecemos que deseamos ver todos los dispositivos

Para empezar tendremos que abrir un terminal pulsando en "Inicio > Ejecutar" (o pulsando en la tecla con el logo de Windows a la vez que la R) y en la casilla resultante escribir "cmd" (sin las comillas) y luego en Aceptar. Se abrirá el terminal de Windows con su característico fondo negro con la línea de comandos lista para recibir nuestra orden. Allí debemos escribir lo siguiente:

```
set devmgr_show_nonpresent_devices=1
```

Este comando establece el parámetro devmgr_show_nonpresent_devices a 1, es decir, lo habilita (por defecto está a 0). A renglón seguido escribimos:

```
start devmgmt.msc
```

Con ello se abre directamente el Administrador de dispositivos (también lo podríamos abrir haciendo clic en "Inicio > Panel de Control > Sistema", seleccionando de la ventana resultante la pestaña "Hardware" y haciendo clic allí sobre el botón "Administrador de dispositivos"). De esta forma se nos facilitará un listado que mediante una estructura jerárquica y desplegable nos permite visualizar los dispositivos que conforman nuestro sistema. Ahora lo que tenemos que hacer es ir al menú "Ver > Mostrar dispositivos ocultos.

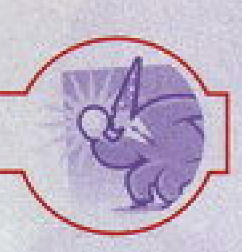
Una vez hecho esto, al desplegar el puerto USB veremos unos dispositivos sombreados que son los distintos periféricos que hemos conectado alguna vez a nuestra máquina. Haciendo clic con el botón derecho y eligiendo en Propiedades accederemos a información adicional que nos permitirá identificarlos mucho más claramente.

Si deseamos dejar el sistema como estaba antes no tenemos más que volver a abrir el terminal tal como se ha explicado anteriormente pero escribir ahora el siguiente comando:

```
set devmgr_show_nonpresent_devices=0
```

Una vez ejecutada la orden se llevarán a cabo los cambios de forma transparente para el usuario y el sistema quedará como estaba antes.

Nicolás Velásquez E.<



Ocultar o mostrar la papelera de reciclaje en Windows

Personalizar nuestro escritorio de Windows sigue siendo uno de los objetivos más perseguidos por todos los usuarios y eliminar o añadir iconos especiales allí es seguramente el punto culminante de cualquier "tuneador" de sistemas que se precie. Y claro, la papelera de reciclaje no podía quedar ajena a estos cambios.

Muchos son los métodos para personalizar nuestro sistema y eliminar el icono de la papelera de reciclaje del escritorio puede considerarse ya como un clásico, aunque nunca hemos hecho mención de cómo hacerlo en esta sección. Por ello, y ya vistos varios métodos, he elegido una forma sencilla y directa que, mediante un procedimiento de dos clics podrá quitar y poner el icono a placer. Para ello vamos a crear un par de archivos de forma que cuando hagamos doble clic sobre ellos realice una serie de cambios en el registro de Windows activando o desactivando la visibilidad del icono.



Cuando hagas doble clic sobre el introducirá la información en el Registro del sistema

Empezaremos creando un documento nuevo con el Bloc de Notas de Windows haciendo clic en "Inicio > Todos los programas > Accesorios > Bloc de notas". Allí copiamos y pegamos el siguiente código:

```
REGEDIT4
[ HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ HideDesktopIcons]
[ HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ HideDesktopIcons\ ClassicStartMenu]
"{ 645FF040-5081-101B-9F08-00AA002F954E} "=dword:00000001
[ HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ HideDesktopIcons\ NewStartPanel]
"{ 645FF040-5081-101B-9F08-00AA002F954E} "=dword:00000001
```

Una vez hecho esto, guardamos este fichero con la extensión "REG", por ejemplo, "QuitarPapelera.reg".

A continuación haz doble clic sobre el nuevo archivo creado, acepta la advertencia inicial y ya se habrán aplicado los cambios aunque si accedes al escritorio comprobarás que la papelera seguirá estando allí, impertérrita. Esto es porque deberá actualizarse a continuación el proceso (denominado "explorer") que es el que regula la visibilidad de iconos en el escritorio. Con el fin de actualizarlo hacemos clic en la combinación de teclas "Ctrl." + "Alt" + "Supr" y de la ventana que se ejecute accedemos a la pestaña "Procesos". Allí buscamos el proceso llamado "explorer.exe", lo seleccionamos y pulsamos en el botón "Finalizar tarea". Verás como el escritorio "desaparece", sólo quedará el fondo de pantalla. Ahora, en la misma ventana accedemos al menú "Archivo > Nueva tarea (Ejecutar)" y escribimos la palabra "Explorer". Automáticamente se producirá un refresco del escritorio volviendo este a su estado original aunque con una pequeña diferencia: el icono de la papelera de reciclaje ya no está.

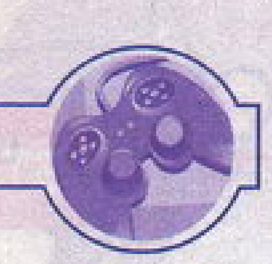
Sin embargo no hemos eliminado realmente nada, simplemente la hemos ocultado y por lo tanto, siempre tenemos la posibilidad de traerla de vuelta. Para ello volvemos a crear un nuevo documento con el Bloc de notas y copiamos el siguiente código.

```
REGEDIT4
[ HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ HideDesktopIcons]
[ HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ HideDesktopIcons\ ClassicStartMenu]
"{ 645FF040-5081-101B-9F08-00AA002F954E} "=dword:00000000
[ HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ HideDesktopIcons\ NewStartPanel]
"{ 645FF040-5081-101B-9F08-00AA002F954E} "=dword:00000000
```

Ahora guardamos este nuevo documento con un nombre como "MostrarPapelera.reg", lo guardamos, lo ejecutamos haciendo doble clic sobre el y refrescamos el escritorio volviendo a terminar y reiniciar el proceso "explorer".

Nicolás Velásquez E.<





Algo nuevo, algo viejo, algo prestado



Con cierto retraso, llega uno de los juegos más esperados de Wii. Esperados para quienes no querían otro entrenador mental ni un port ni un arcade simplón que hiciera uso del wiimando. Zack & Wiki: En busca del Tesoro de Barbaros, sin ser algo terriblemente original, es uno de los mejores juegos actualmente para la consola de Nintendo, por su particular mezcla de elementos muy conocidos en un estupendo "point & click", con todo el sabor de las aventuras gráficas clásicas.

Capcom ha preparado un festín de rompecabezas con ambiente pirata y estilo cartoon. Zack es un joven aspirante a pirata con cierta obsesión por el chocolate, y siempre va acompañado por una criatura voladora algo chillona, algo así como un mono, llamado Wiki. Juntos descubren casi por accidente que el tesoro del mítico pirata Barbaros está repartido por todo el mundo. Ávido de fama y popularidad, Zack acepta ir a buscar todos los tesoros de Barbaros, el pirata más conocido y temido, cuyo espíritu esconde no pocos secretos que iremos descubriendo poco a poco. Cada pieza del tesoro de Barbaros es un rompecabezas, una fase en la que tendremos que accionar determinados ingenios y usar ciertos objetos para abrir los preciados cofres.

Zack & Wiki: En busca del Tesoro de Barbaros es una aventura "point & click" de toda la vida, solo que con el wiimando en nuestras manos. Podremos ver el mapeado de cada escenario y apuntar donde queramos desplazar a Zack, así como apuntar a los objetos y personajes con que queremos interactuar. El control, no podía ser de otra forma, es extremadamente intuitivo, pero más de una vez nos dará problemas de respuesta. O sea, es fácil controlar a Zack y sus acciones, pero a veces podemos encontrarnos maldiciendo en lenguas por algún que otro desajuste.

Además del clásico control de las aventuras gráficas, en determinados momentos el juego cambiará la vista a primera persona. Sobre todo, para activar dispositivos o máquinas, o usar ciertos objetos. Ahí es donde el wiimando cobra protagonismo más allá del mero "point & click". Por ejemplo, para derribar un enorme bloque de hielo que se encuentra sobre un cofre congelado tendremos que usar un taladro, un carámbano afilado, una bomba y una sierra. Cada objeto se maneja de forma distinta gracias al wiimando. La mayoría de objetos se consiguen de una forma muy original. Cuando nos encontremos con ciertos animales, agitaremos el mando y el leal Wiki convertirá esos animales en herramientas. Si lo agitamos de nuevo volverán a su forma animal, que también necesitaremos en más de una ocasión para ciertos cometidos.

Los puzzles son variados en cuanto a dificultad y desarrollo. Aunque se repiten los objetos no se repiten los rompecabezas ni los desafíos, cosa que se agradece. Muchos de esos puzzles conllevan un número limitado de intentos o un límite de tiempo para llevarlo a cabo. Además de las piezas que componen el cuerpo/tesoro del pirata Barbaros, hay otras sorpresas a lo largo del camino de Zack y Wiki.

Puede decirse que Capcom ha acertado de pleno en esta nueva apuesta para Wii. El juego rescata elementos de las aventuras gráficas, los combina con una estupenda ambientación, mucho humor y lo corona con un buen control. Se agradece horrores que Capcom haya elegido otros derroteros en una época en la que muchas compañías van a lo fácil en Wii. Muy recomendable.







	7
	7
	7
	8
	8
total	8

gráficos · sonido · rapidez · jugabilidad · adicción



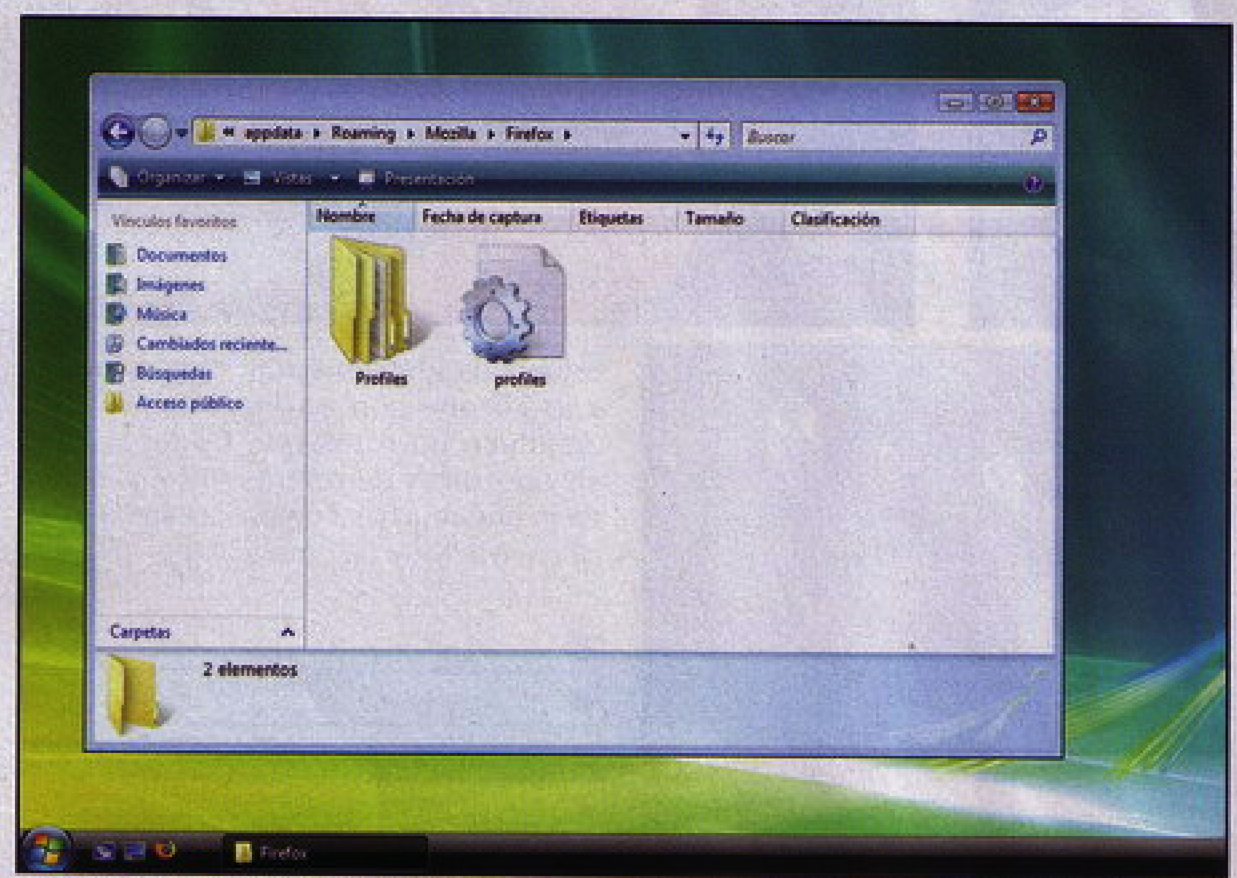
Borrar el perfil de Firefox en Windows Vista

La aparición de Windows Vista en el mercado ha traído toda una serie de novedades que, aunque no sean del gusto de muchos, se afianzan poco a poco demostrando que es necesario comenzar a descubrir sus interioridades con el fin de optimizar su funcionamiento con determinadas aplicaciones como Firefox.

Desde que Windows Vista hiciera su aparición hace ya algunos meses son muchos los que ya utilizan este sistema operativo que está llamado a ser el estándar a seguir visto la apuesta que por él ha hecho Microsoft (su kernel es el que incorporará Windows Server 2008 y se incluirá en la mesa táctil Surface, entre otros). Los usuarios nos hemos encontrado con una arquitectura totalmente renovada y asimismo, acostumbrados a Windows XP, muchas dudas sobre cómo realizar tal o cual tarea. Y qué decir de aplicar trucos para realizar funciones más específicas.

Aunque haya salido Internet Explorer 7 con muchas mejoras, Firefox sigue siendo la elección de un gran número de usuarios a la hora de navegar por la red (de hecho Firefox 2.0.0.2 ha sido anunciada como la primera versión de esta aplicación en soportar Windows Vista, corrigiendo numerosos fallos aparecidos en versiones anteriores). Tenemos así que por ejemplo que apartados como la gestión de perfiles en el navegador de Mozilla cambia sustancialmente bajo Vista.

Si varias personas comparten el mismo ordenador (en sesiones independientes, por ejemplo), o si mantienes distintos intereses de navegación (trabajo y aficiones por ejemplo) es muy útil disponer de distintos perfiles de usuario, cada uno con su propia identidad, favoritos y preferencias. Esto resulta de mucha utilidad en tu hogar para los niños o en el trabajo, por ejemplo. Asimismo, estos perfiles te permiten conservar una serie de datos como los favoritos y otros aspectos del navegador que por defecto se mantendrán inalterables cuando desinstales el navegador Firefox de tu sistema operativo y vuelvas a descargar e instalar otra versión, o la misma si fuera necesario. El truco está en que tu perfil se encuentra almacenado en Vista en un lugar distinto y permanece seguro a pesar de que desinstales el navegador. La carpeta del perfil es el lugar donde se guardan todas las preferencias del programa, y es interesante que conozcas su ubicación para poder hacer una copia de seguridad o borrarlo, que es nuestro caso.



ocaliza la carpeta con los perfiles de Firefox

Para eliminar todo rastro de una instalación anterior de Firefox en Windows Vista comienza eliminando el programa con el desinstalador que el programa trae por defecto, y al que podrás acceder fácilmente desde el Panel de Control con la opción de desinstalar programas, similar al existente en otras versiones de Windows. Una vez hecho esto será necesario que localices en qué lugar se encuentra tu perfil para también deshacerte de el (de esta forma te asegurarás un borrado limpio y completo). Con esta premisa deberás localizar la siguiente carpeta en tu disco duro:

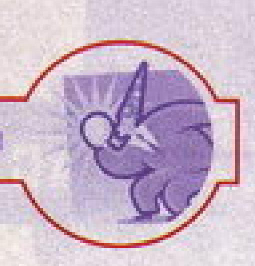
```
C:\Usuarios\[ Nombre de usuario] \DataRoaming\Mozilla\Firefox\Profiles\
```

También puedes hacer uso del cuadro de búsqueda de Windows Vista para encontrarlo directamente. Para ello basta con hacer clic en el botón Inicio y en el cuadro de búsqueda tecleamos "Appdata" (sin las comillas). A continuación abre la carpeta que aparece en los resultados pulsando sobre el resultado encontrado con el ratón.

Lo que debes hacer ahora es localizar tu perfil. Ten en cuenta que el perfil no se encuentra almacenado en la carpeta Local, a pesar de contar dentro con una subcarpeta de Firefox. Será necesario que busques la carpeta Mozilla y en su interior el subdirectorio Firefox, bajo el directorio Roaming. En esta carpeta ya puedes buscar tu perfil que podrás borrar fácilmente haciendo clic sobre la carpeta y pulsando en la tecla suprimir del teclado. Tan solo debes recordar que a partir de ahora la nueva instalación de Firefox que efectúes será totalmente nueva, sin datos previos almacenados.

Finalmente, si lo que deseas en lugar de borrar el perfil es copiarlo a otro equipo, tan sólo tienes que copiar esos archivos y llevarlos al perfil nuevo. Como es lógico, para cualquier cambio de este tipo será necesario que dispongas de derechos de administrador.

Nicolás Velásquez E.<



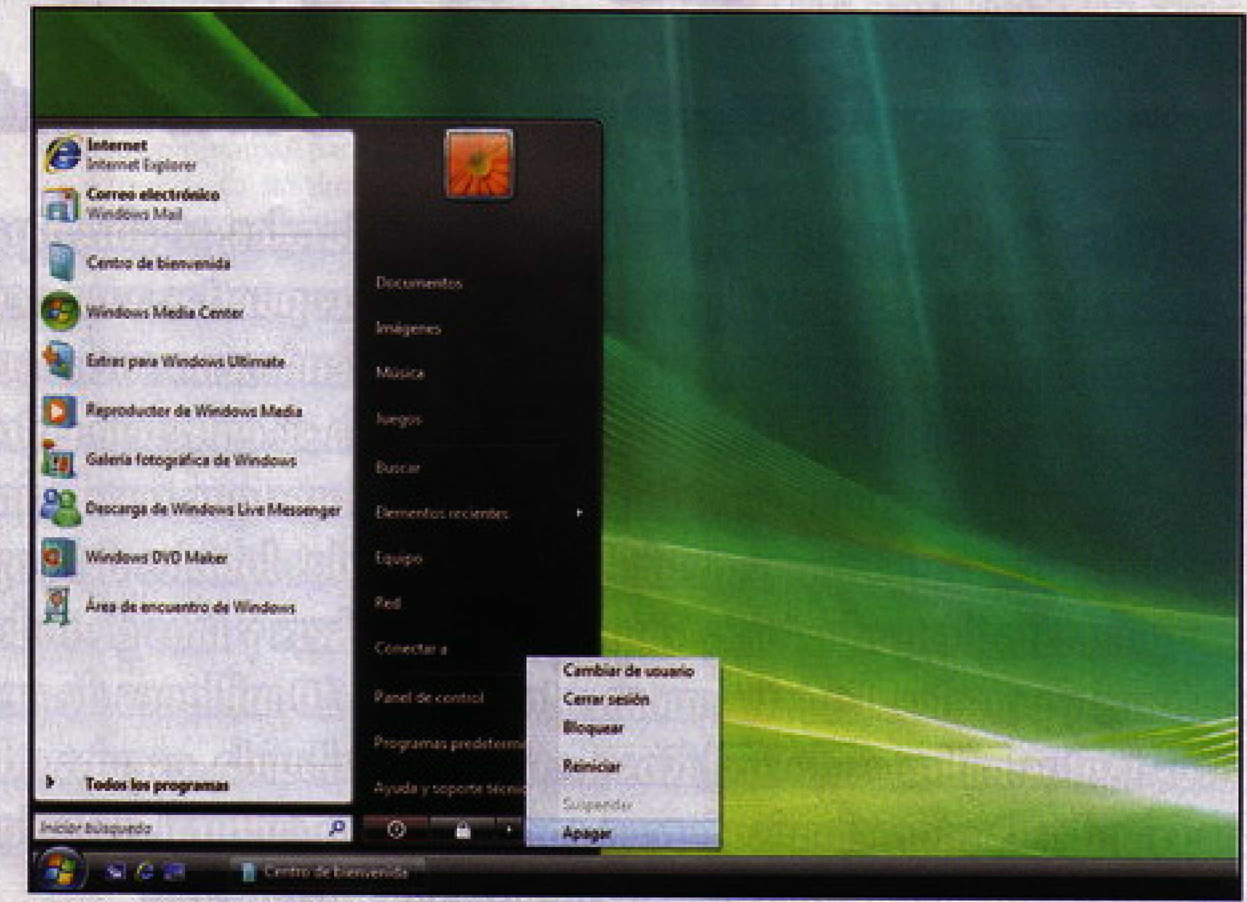
Poner el botón de apagado en el menú

Apagar un equipo suele ser una tarea inmediata, rápida, en la que muy pocos pensamos... hasta que nos plantea algún contratiempo. Desde que apareció Windows Vista, el sistema de apagado no es exactamente el mismo que con XP y muchos lo habrán notado, aunque con unos pocos ajustes todo puede quedar como antes.

La aparición de Windows Vista en el mercado internacional ha generado todo tipo de acaloradas discusiones en pro y en contra del sistema operativo que viene a reemplazar a Windows XP. Sin embargo, de forma objetiva, lo que no se puede negar es que supone un cambio bastante importante tanto desde el punto de vista conceptual como funcional.

Un renovado aspecto gráfico abanderado por el llamativo efecto Aero y nuevas aplicaciones son quizás los aspectos que más llaman la atención en un principio. Con todo, el usuario que se adentre un poco en su uso descubrirá rápidamente que hay muchos más alteraciones que tienen que ver con el uso más básico del sistema y que por ende afectará a cualquier usuario, no sólo los más avanzados. Y de ahí que una acción tan sencilla como el proceso de apagado, cuando se trata de un equipo portátil, no sea tan inmediato y expeditivo como lo era antes.

Con Windows XP bastaba con ir al menú "Inicio > Apagar equipo" para que el sistema se cerrara (previa selección del tipo de cierre) pero si ahora pretendemos realizar el mismo proceso en Windows Vista esto nos llevará directamente a una Suspensión de sistema que, no dudamos, tiene sus indudables ventajas (un reinicio infinitamente más rápido aunque con un consumo reducido y continuado de la batería), pero que a la postre no es un apagado en toda regla. En un sistema Vista, si lo que queremos es apagar del todo nuestro sistema, tendremos que ir un paso más allá, desplegando un nuevo listado de opciones desde este punto donde se nos ofrecerán todas las opciones de apagado posibles, tras lo cual podremos seleccionar luego del menú desplegado la opción "Apagar".



En Vista el Apagado es en realidad una Suspensión

Para usuarios acostumbrados al clásico método de apagado, esto puede suponer un engorro añadido que, como veremos, nos será muy fácil subsanar, todo ello gracias a una sencilla configuración que nos permitirá cambiar ese acceso directo de manera que se apague completamente el sistema, tal y como lo hacía en XP.

Para empezar debemos dirigirnos al Panel de control haciendo clic en la secuencia "Inicio > Panel de control" y allí seleccionamos el apartado "Sistema y Mantenimiento" pulsando sobre este. Además de muchas otras opciones, en el menú situado en el lateral izquierdo de esta ventana será posible elegir el modo en que deberá comportarse el botón de Encendido desde el enlace "Elegir el comportamiento del botón de encendido". Como curiosidad también podremos ver por ejemplo un acceso directo para "Cambiar la frecuencia con la que el equipo entra en estado de suspensión".

Si hacemos clic en el primero de ellos nos dirigiremos directamente a una nueva pantalla desde la que se nos permitirá configurar los botones de encendido y activar la protección con contraseña, entre otras cosas. De esta guisa nos será posible elegir el plan de energía deseado para nuestra máquina, teniendo en cuenta que todos los cambios realizados en esta configuración se aplicarán a todos los planes de energía (un dato fundamental del que seguramente estará al tanto cualquier usuario que utilice habitualmente un dispositivo portátil).

En el apartado central "Configuración de los botones y la tapa de encendido y de suspensión" encontramos varios listados desplegables para las situaciones en las que utilicemos el equipo con batería o conectado a la corriente. Desde aquí podremos configurar el comportamiento a nuestro gusto y si lo que deseamos es que se apague el equipo bastará con seleccionar la opción "Apagar equipo" en cada caso.

Una vez hecho esto, pulsamos en el botón "Guardar cambios" situado en la parte inferior y ya tendremos nuestro botón de apagado configurado a nuestro gusto tal como estábamos acostumbrados en Windows XP.

Nicolás Velásquez E.<

p2p, de igual a igual

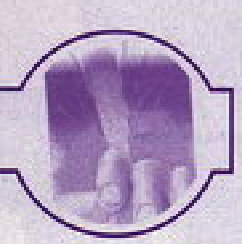
Copyratas en el océano de la materia negra

Las redes p2p, la pesadilla de las industrias culturales, se abren paso como un tsunami tecnológico y cultural que arrasa con el pasado para abrir las puertas a un océano abierto e imprevisible. Sin embargo las entrañas y los engranajes de este fenómeno social se resisten a una comprensión fácil. La complejidad de la mal llamada piratería se entreteje entre el anonimato masivo, pequeñas empresas que gestionan servidores, programadores que revolucionan los protocolos de intercambio y la amenaza permanente de los desesperados lobbies del copyright. Pero, sobre todo, las comunidades de traductoras, rippeadores, crackers y fans de todo tipo que se organizan alrededor de foros y portales. En estos momentos más de 20 millones de personas están intercambiando otros tantos millones de archivos de forma distribuida, esquivando el control y la mediación que las grandes corporaciones ejercen contra el flujo cultural. ¿Quién está detrás de todos esto? ¿Cómo, cuándo y dónde surge esta imparable revolución?

La materia negra

Vivimos en una internet de masas mucho más centralizada de lo fue en sus orígenes. La inmensa mayoría de las usuarias son pasivas consumidoras de tráfico, sometidas al rol de clientes de multitud de servidores centralizados que ofrecen servicios de correo, ftp, video, etc. Los servidores son núcleos de control y acumulación. Eso supone desaprovechar la capacidad de una red real. Se denomina "materia negra" al ancho de banda, la memoria y la capacidad de procesamiento desaprovechado de todos los clientes (es decir de nuestros ordenadores). Pero la vieja ARPANET se diseñó como un sistema completamente distribuido y capaz de conectar personas sin mediadores. Por eso la arquitectura básica de internet permite darle la vuelta al flujo actual, usar la red para conectar a iguales, construyendo red en la materia negra. Eso son las redes p2p, abreviatura del peer to peer que viene a significar "de igual a igual" o "entre pares", redes de intercambio directa de información sin que medie un servidor intermedio (aunque a veces se hace uso de servidores para realizar búsquedas y conectar a las usuarias).





Sus orígenes ser remontan al primer informe RFC de la Internet Engineering Task Force1, allá por 1969. Hoy en día diversos protocolos y programas permiten crear redes p2p para usos diversos; desde la mensajería instantánea (Jabber) hasta los servidores de nombres de dominios (DNS) pasando por wikis distribuidos (Buzm2). Pero, sin duda, las redes entre iguales han saltado a la fama por la capacidad que tienen de gestionar tráfico muy pesado sin un control central y permitiendo cierto nivel de anonimato. Eso es lo que ha hecho de las redes p2p un océano de materia negra en el que se está creando un tsunami de intercambio de archivos (música, películas, libros) al margen de la propiedad intelectual.

Tecnologías del intercambio

Napster fue la red que marcó el comienzo de las p2p de masas. Su creador, Shawn Fanning, quería facilitar la búsqueda y descarga de música en la red. Tras varios meses picando código nació Napster. Era el año 1998 y el invento, pero sobre todo su éxito, pilló por sorpresa a la industria. Un año después la banda Metallica, junto a la RIAA (la SGAE norteamericana) demandó a su creador. Gracias a la repercusión mediática de la demanda, en febrero del 2001 Napster contaba ya con más de 26 millones de usuarios. Pero en Junio del 2001 cerraba por orden judicial. La historia de Napster marcaría ya las polémicas que desde entonces rodearán a las redes p2p. Mientras que los fans de Metallica se echaban encima del grupo por denunciar esta arquitectura del intercambio, la banda Radiohead daba su apoyo incondicional, después de que su último disco alcanzara el top 20 en los EEUU gracias al intercambio masivo. Después vinieron Audiogalaxy y Kazaa que también cerraron o se replegaron por culpa de las demandas de las sociedades de gestión.

El caso Napster pasará sobre todo a la historia como escarmiento para los intentos de control de la industria. Su cierre judicial fue el pistoletazo de salida para el surgimiento de muchas otras redes p2p. Y el mensaje para la industria cultural quedó claro: el fenómeno del intercambio masivo de archivos era imparable. Poco después del caso Napster, un programador español, Pablo Soto, saltaba a la fama, con apenas 24 años, al desarrollar un protocolo para redes p2p (llamado MANOLITO) que parecía blindado a cualquier tipo de demanda judicial. Sin depender de servidores centrales, MANOLITO guardaba el anonimato de los usuarios y el contenido de los archivos compartidos. Recientemente, Pablo de Soto se ha volcado a desarrollar Omemo3, un sistema libre (MANOLITO sigue siendo propietario a día de hoy) que permite crear un gigantesco disco duro distribuido entre todo el que participe de la red.

Existen decenas de protocolos p2p y otros tantos clientes fáciles de instalar. Las redes montadas sobre los protocolos eDonkey (la famosa Mula) y Bittorrent son los más utilizados, con sus respectivos clientes como el eMule y el aMule para la red eDonkey o el BitTornado para Bittorrent. Pero entre los programas para conectarse a redes p2p destaca sin duda el MLDonkey4, desarrollado por dos programadores franceses, Fabrice Le Fessant5 y Simon Patarin6 del Instituto Nacional Francés de Investigación en Informática y Automática. MLDonkey fue el primero en permitir un control remoto a través de una interfaz web y es uno de los más populares, completamente libre (con licencia GPL) y multiplataforma (funciona en GNU/Linux, Windows, y Mac). Pero además, MLDonkey fue el primer cliente multired capaz de conectarse a las redes más importantes: como eDonkey, Bittorrent, Gnutella, Overnet y un largo etcétera. Si una red cae, MLDonkey puede seguir descargando y subiendo contenido en otras redes.

Cultivando cultura

Diversos foros y portales permiten que grupos anónimos de usuarias se reúnan alrededor de ciertos temas para compilar y organizar colecciones completas de películas, libros o música. El grupo Freakyflicks7, por ejemplo, ha comprimido y etiquetado alrededor de un millar de películas clásicas y de culto, como una entrevista a Woody Allen dirigida por el mismisimo Jean Luc Godard, imposible de encontrar en ninguna tienda especializada en cine. No es ninguna tontería. El 80% de las películas mudas (rodadas a principios del siglo pasada) se ha perdido para siempre por culpa de unas leyes de copyright que, prohibiendo su copia y reproducción, hicieron que el caduco soporte del celuloide se marchitara hasta borrarlas definitivamente de la historia. Gracias a las redes p2p, muchas películas marginales (y no por ello de menor calidad que los últimos estrenos de Hoolywood) se mantienen accesibles y vivas en la red. Otro ejemplo destacable es la web Rebelmule8 que resumen e indexa multitud de documentales de carácter social (prácticamente imposibles de encontrar en videoclubs o en la propia televisión).

No podemos olvidar uno de los fenómenos más interesantes que han generado las redes p2p. Se trata de la distribución y subtitulado de series norteamericanas, de forma casi inmediata (apenas unas horas después de ser emitidas en los EEUU) y realizadas, sin ánimo de lucro, por los propios fans de las series. Pero no todo son películas y música. Una de las colecciones más sorprendentes que ofrecen las redes p2p es una compilación de miles de libros de texto en formato pdf. Se trata de un total de 7 DVDs bajo el título "Great Science Textbooks DVD Library 2007". Quién ha conseguido reunir semejante biblioteca es todo un misterio, pero seguro que las estudiantes de cientos de universidades del tercer mundo agradecen poder acceder a un conocimiento que, de otro modo, les costaría más del sueldo medio anual en su país (a una media de unos 100$ el libro de texto en papel).

Desgraciadamente las colecciones de películas clásicas y de libros de texto académicos son más bien una excepción, la inmensa mayoría de archivos que circulan por la red son los "éxitos" de la industria. Más de uno piensa que la verdadera revolución vendrá cuando las nuevas tecnologías permitan no sólo la difusión sino la modificación y creación de nuevas obras fuera de los circuitos comerciales. Esa revolución ya ha comenzado y se está difundiendo como la pólvora por las redes p2p. La Liga de los Nobles Pares, un colectivo anónimo de creadores audiovisuales, acaba de sacar la segunda parte del documental "Steal This Film"9 (roba esta película), todo un éxito en las redes p2p. Aunque cuidado, el documental tiene copyright. Sólo para que te des el gusto de saltártelo...

La bahía pirata y otros archipiélagos rebeldes

El primer documental de la Liga de los Nobles Pares trata sobre el nacimiento y los problemas legales de The Pirate Bay, uno de los sitios web más populares para buscar enlaces de la red Bittorrent. El segundo, más teórico, explica porqué esta revolución es imparable y cómo sus dimensiones han superado con creces el mero "todo es gratis". Hace poco The Pirate Bay batía un nuevo record: 10 millones de usuarios y más de un millón de archivos compartidos. Es el sitio web más popular de la red Bittorrent, pero también es mucho más. A diferencia de otros servidores y buscadores p2p, este proyecto nació y se consolidó como apuesta política, sin intención de sacar dinero (más allá del necesario para mantener el tráfico en su web) y con una desvergonzada apuesta mediática enarbolando la bandera pirata.

Asentada en Suecia The Pirate Bay forma un verdadero triángulo de las Bermudas

junto a Piratbyran10 (la oficina pirata sueca) y el Partido Pirata11. En mayo del 2006 sufrió su primera amenaza seria. Tal y como explican en el documental, el lobby norteamericano MPA (Motion Picture Association—una especie de SGAE de la industria del cine) había presionado a las autoridades norteamericanas para que a su vez presionaran seriamente a las autoridades suecas: la bahía pirata tenía que desaparecer del mapa. El ataque del imperio mercantil del copyright fue un abordaje en toda regla. La policía sueca se llevó 300 servidores (de los cuales sólo 20 eran del sitio thepiratebay.net) y lo hizo sin orden judicial. La noticia saltó rápidamente a la red, pero también a los medios de comunicación suecos. El efecto del abordaje de los lobbies de la industria americana fue el contrario al esperado. The Pirate Bay obtuvo una atención mediática espectacular y se produjeron manifestaciones masivas por todo el país (más de 5 partidos políticos suecos enviaron a sus representantes para apoyar a los piratas). En tres días el sitio volvía a funcionar con total normalidad y la afiliación al partido pirata sueco se duplicó en menos de dos días.

Aunque The Pirate Bay se enfrenta ahora a la acción de la fiscalía sueca (habrá que ver el resultado) los efectos de defender la "piratería" como proyecto político se abren paso cada vez con más fuerza. Los partidos verdes europeos se acaban de posicionar abiertamente a favor del libre intercambio de archivos con campaña mediática incluida títulada "Yo no robaría ... pero compar-



El atrevido logotipo de The Pirate Bay, el servidor más popular de la red de intercambio de archivos Bittorrent. The Pirate Bay, junto a la Oficina pirata y el Partido Pirata (todos ellos suecos), forma un vanguardista movimiento social y político en favor del intercambio de archivos.

to"12. Lo que empezó en manos de jóvenes programadores entusiasmados por explorar las posibilidades de internet y la pasión por la música ha terminado siendo un fenómeno social y político sin precedentes. Según el último informe de la LFPI13 (la federación internacional de la industria fonográfica) las descargas libres (ellos las llaman ilegales) sobrepasan a las descargas de pago en proporción de 20 a 1. Impedir y reprimir la potencia inmediata del intercambio directo es como vallar la costa oceánica para dejar sólo un estrecho pasillo de acceso (y cobrar cada baño en el mar a 25€ la hora y media que es lo que dura un DVD). Pero las tecnologías p2p han permitido sortear los obstáculos artificiales que el negocio de la propiedad intelectual ha impuesto sobre la cultura. Y esta revolución no exige sacrificios humanos, guillotinas o fusilamientos. Basta con seguir sembrando cultura en las redes. Y dejar que fluya los torrentes hacia un océano de abundancia.

EVhAck (evhack.info@gmail.com)

Referencias

[1] http://tools.ietf.org/html/rfc1
[2] http://www.buzm.com/
[3] http://www.omemo.com/
[4] http://mldonkey.sourceforge.net
[5] http://www.lefessant.net/
[6] http://patarin.info/
[8] http://biblioweb.sindominio.net
[9] http://www.freakyflicks.tk/
[10] http://www.nodo50.org/rebeldemule/
[11] http://www.stealthisfilm.com
[12] http://piratbyran.org/
[12] http://www.pp-international.net/
[14] http://iwouldntsteal.net/
[15] http://www.ifpi.org/content/library/DMR2008.pdf

Ellos son los responsables del éxito de muchas personas.

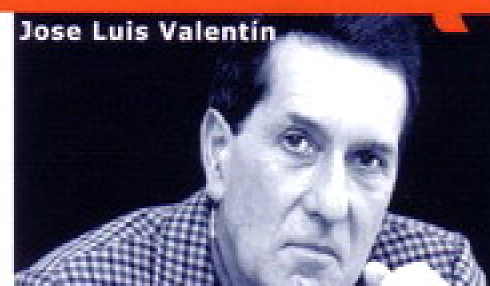
Son los directores de las diferentes áreas de **CCC Profesional**.
Gracias a ellos más de 85.000 personas han salido adelante profesionalmente en los últimos tres años.
Ellos también están para ayudarte a ti a asegurar tu futuro profesional haciendo los cursos prácticos y fáciles.
Cuentas con su respaldo y la Garantía de CCC.

CCC profesional
902 20 21 22
www.cursosccc.com

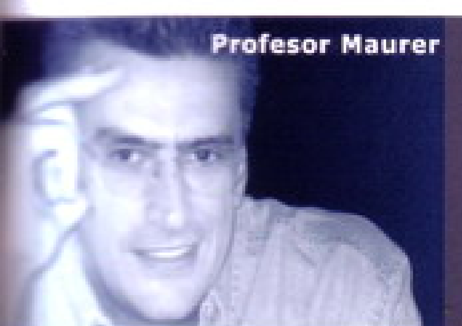


ACCESO A ESO Y UNIVERSIDAD
- Preparación al Título Oficial de Graduado ESO.
- Acceso a la Universidad para Mayores de 25 años.





PROFESIONES TÉCNICAS
- Técnico en Instalaciones de Energía Solar Térmica.
- Instalador Electricista. FP
- Técnico en Construcción de Obras.
- Título Oficial de Tco. Sup. en Prevención de Riesgos Laborales.
- Profesor de Educación Vial.



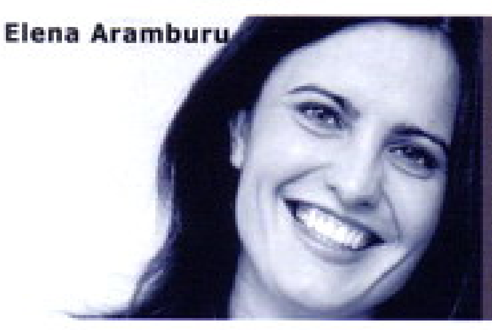
IDIOMAS
- El Inglés con Mil Palabras. The Maurer Method.
- Chino con la profesora Yang Yun.



PROFESIONES SANITARIAS
- Auxiliar de Enfermería. FP
- Auxiliar de Geriatría.
- Auxiliar de Jardín de Infancia.
- Auxiliar de Farmacia. FP



BELLEZA Y MODA
- Esteticista Profesional. FP
- Peluquería. FP
- Diseño de Moda.



EMPRESA E INFORMÁTICA
- Microsoft Office Formación Personalizada.
- Título Oficial de Agente Comercial.
- Administración de Empresas.
- Gestor Inmobiliario.
- Experto en Bolsa e Inversiones.
- Tco. Superior en Secretariado. FP
- Técnico en Contabilidad.
- Técnico en Diseño Web.
- Tco. en Protección de Datos y Seguridad Informática.



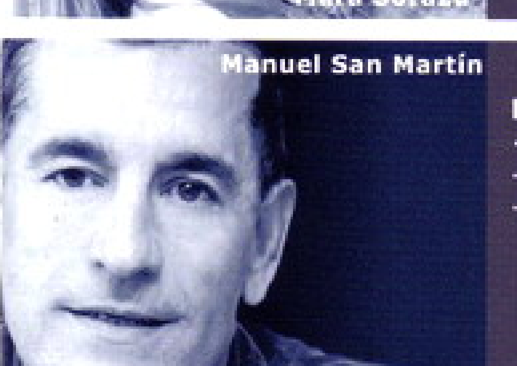
MEDICINAS COMPLEMENTARIAS
- Monitor/a de Relajación y Desarrollo Personal.
- Diploma en Naturopatía.
- Profesor/a de Yoga.
- Quiromasajista (MDF).
- Quiromancia: La Lectura de la Mano.



VETERINARIA
- Auxiliar de Clínica Veterinaria.
- Adiestramiento de perros.
- Peluquería y Estética Canina.



ARTES, DECORACIÓN Y HOSTELERÍA.
- Decoración.
- Monitor/a de Manualidades.
- Curso Práctico de Tapicería.
- Cocinero/a Profesional.
- Técnico de Gestión de Empresa de Hostelería.



PROFESIONES DEPORTIVAS
- Instructor de Pilates.
- Monitor/a de Preparación Física.
- Monitor/a de Aerobic y Fitness.

Saca la profesión que llevas dentro



Matricúlate este mes y consigue GRATIS esta estupenda AGENDA ELECTRÓNICA

☐ Sí, deseo recibir información (*)

¿DE QUÉ CURSO TE INTERESA RECIBIR INFORMACIÓN SIN COMPROMISO? ....

Nombre: .... Apellidos: ....
E-mail: ....
Teléfono/s: ...... / ...... Fecha nacimiento: ... / ... / ...
Domicilio: .... Nº: ...... Piso: ......
Población: .... C.P: ...... Provincia: ....
DNI (opcional): .... País de nacimiento: ....

Infórmate en el
902 20 21 22
www.cursosccc.com
o envía este cupón a **CCC**: Apdo. 17222 - 28080 Madrid.









